NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AN APPROACH TO VULNERABILITY ASSESSMENT FOR NAVY SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYTEMS

by

Dennis Hart

September 2004

Thesis Advisor:	Cynthia E. Irvine
Co-Thesis Advisor:	Karen Burke

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: : An Approach to Vulnerability Assessment for Navy Supervisory Control and Data Acquisition (SCADA) Systems			**5. FUNDING NUMBERS**
6. AUTHOR(S) **Hart, Dennis J**			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Department of the Navy Chief Information Officer Presidential Towers Suite 2100 2511 Jefferson Davis Hwy, Arlington, VA 22202			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The unfortunate events of September 11, 2001 have caused a renewed effort to protect our Nation's Critical Infrastructures. SCADA systems are relied upon in a large number of the sectors that make up the critical infrastructure and their importance was reinforced during the massive power outage that occurred in August 2003.

Growing reliance upon the Internet has emphasized the vulnerability of SCADA system communications to cyber attack. Only through diligent and continuous vulnerability assessment and certification and accreditation of these systems will the United States be able to mitigate some of the vulnerabilities of these systems. A case study presented here has validated the need for continued focus in this area.

This thesis consolidates some of the research that has already been done in the area of SCADA vulnerability assessment and applies it by developing an initial vulnerability assessment checklist for Department of the Navy systems. This checklist can and should also be used in the certification and accreditation of DoN SCADA systems.

A promising technology was also discovered during this research that should be explored further to secure SCADA communications. This will be touched on briefly.

14. SUBJECT TERMS Vulnerability Assessment, SCADA, Information Assurance, Supervisory Control and Data Acquisition			**15. NUMBER OF PAGES** 182
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

AN APPROACH TO VULNERABILITY ASSESSMENT FOR NAVY SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEMS

Dennis J Hart
Major, United States Marine Corps
B.S., Chapman University, 1994

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 2004

Author: Dennis J. Hart

Approved by: Dr. Cynthia E. Irvine
Thesis Advisor

Karen Burke
Co-Advisor

Dr. Peter J. Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The unfortunate events of September 11, 2001 have caused a renewed effort to protect our Nation's Critical Infrastructures. SCADA systems are relied upon in a large number of the sectors that make up the critical infrastructure and their importance was reinforced during the massive power outage that occurred in August 2003.

Growing reliance upon the Internet has emphasized the vulnerability of SCADA system communications to cyber attack. Only through diligent and continuous vulnerability assessment and certification and accreditation of these systems will the United States be able to mitigate some of the vulnerabilities of these systems. A case study presented here has validated the need for continued focus in this area.

This thesis consolidates some of the research that has already been done in the area of SCADA vulnerability assessment and applies it by developing an initial vulnerability assessment checklist for Department of the Navy systems. This checklist can and should also be used in the certification and accreditation of DoN SCADA systems.

A promising technology was also discovered during this research that should be explored further to secure SCADA communications. This will be touched on briefly.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to express thanks to many individuals without whom the completion of thesis would not be possible.

I give thanks to my wife and children without whom I would be incomplete. Although sometimes a distraction, your presence provided me with the motivation I so desperately needed through the entire thesis process.

I would also like to thank my parents, Carlis and Jeanette Hart, for instilling in me the core values that have always guided my way.

I would like to thank Dr. Cynthia Irvine, Deborah Shifflett, and Karen Burke, my advisory team. Thank you for your patience and assistance and dedication. I would also like to acknowledge Dr. George Dinolt for reading and commenting on the finished thesis.

I would also like to thank Gary Kreeger, Jean Brennan, and Patty Walker for your absolutely fantastic job of supporting me as a student through my academic career at NPS.

Finally, I would like to thank my Lord and Savior Jesus Christ for molding me into the person that I am. I give thanks to Him for the many blessings that He has bestowed upon me.

This research was supported by the Department of the Navy Chief Information Officer with special thanks to Colleen Herrmann.

THIS PAGE INTENTIONALLY LEFT BLANK

GLOSSARY

AP	Access Point
CIP	Critical Infrastructure Protection
C & A	Certification and Accreditation
CIDX	Chemical Industry Data Exchange
CND	Computer Network Defense
COTS	Commercial off the Shelf
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DITSCAP	Department of Defense Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
DoN	Department of the Navy
DOS	Denial of Service
HMI	Human Machine Interface
HSPD	Homeland Security Presidential Directive
HVAC	Heating, Ventilation, and Air-Conditioning
ICS	Industrial Control System
IED	Intelligent Electronic Device
IP	Internet Protocol
INEEL	Idaho National Engineering and Environment Laboratory
IT	Information Technology

ISA	The Instrumentation, Systems and Automation Society
LAN	Local Area Network
NERC	North American Electric Reliability Council
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NIVA	Naval Integrated Vulnerability Assessment
NSA	National Security Agency
PCSRF	Process Control Security Requirements Forum
PDD 63	Presidential Decision Directive 63
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SSAA	System Security Authorization Agreement
VPN	Virtual Private Network
WAN	Wide Are Network

I. INTRODUCTION

A. THESIS STATEMENT

Supervisory Control and Data Acquisition (SCADA) systems are being employed throughout the DoD/DoN. In the Government sector, such systems have been recognized by the FBI and the Department of Homeland Security as a serious concern in efforts to protect the Nation's Critical Infrastructure. DoN Vulnerability Assessment teams have acknowledged a need to include SCADA systems as part of their facility assessment process. This effort is in its infancy and a more thorough understanding of the threats and vulnerabilities that SCADA systems expose the DoD/DoN to and what can be done to mitigate them is needed.

This work identifies the common components make up a SCADA system and the information security vulnerabilities that exist within these systems. Current industry and Government documents in this area of research will be reviewed and analyzed as part of this study. Using this information, a preliminary checklist for vulnerability assessment of DoN SCADA systems was created. An assessment of an operational SCADA system was conducted. This permitted validation and revision of the preliminary checklist.

B. THESIS SCOPE AND ORGANIZATION

This research was to result in the development of a preliminary checklist for vulnerability assessment of DoN SCADA systems to be used by DoN Vulnerability Assessment Teams. As part of the research, a SCADA demonstration system was built. That system and an existing commercial SCADA system that is representative of the systems that the DoN is dependent upon was used to validate the checklist.

The thesis chapters are organized as follows:

Chapter I - Introduction – This chapter introduces SCADA systems and their importance and explains the motivation behind this work

Chapter II - Background – This chapter provides background material that motivates the research. Additionally it provides examples of where SCADA systems can be found and why they are of interest to the DoN.

Chapter III – Vulnerability Assessments – This chapter discusses the rationale for the preliminary checklist, explains what a vulnerability assessment seeks to accomplish and lists some to the items to be covered in an assessment.

Chapter IV – Developing and Validating a Vulnerability Assessment for SCADA Systems Test Plan – This chapter describes the case study conducted to develop and validate the preliminary checklist.

Chapter V - Recommendations and Conclusions – This chapter summarizes the conclusions reached and makes recommendations for future work.

II. BACKGROUND

Process or Industrial Control Systems (PCS/ICS) have been in use since the 1960s and are often broadly categorized as Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) systems. DCS are used to control large, complex processes but typically at a single site. SCADA systems are used to control more dispersed assets, hence there is increased concern about their cyber security, especially where centralized data acquisition is as important as control. Presidential Decision Directive 63 considers these as critical infrastructure components and a SCADA system under the control of an adversary could wreak national havoc. The Department of Homeland Security recently recognized the need to protect against the vulnerabilities that exist in SCADA systems by funding 11 small business research grants that deal with developing technologies that will help to secure these systems. [DHS]

SCADA systems are employed throughout industry and are used to monitor and control processes and functions that affect our nation's critical infrastructure. The Department of Defense (DoD) and the United States as a whole is very reliant upon and is a major consumer of the products and services that are managed by SCADA systems. Some of these industries are the electric, oil, gas, chemical manufacturing, transportation, and waste water.

A. SCADA COMPONENTS

Figure 1 shows the components of a SCADA system. Theses components are: the controller, sensors, actuators (or final control elements),a human machine interface (HMI) and a remote diagnostics and maintenance capability [SPP].

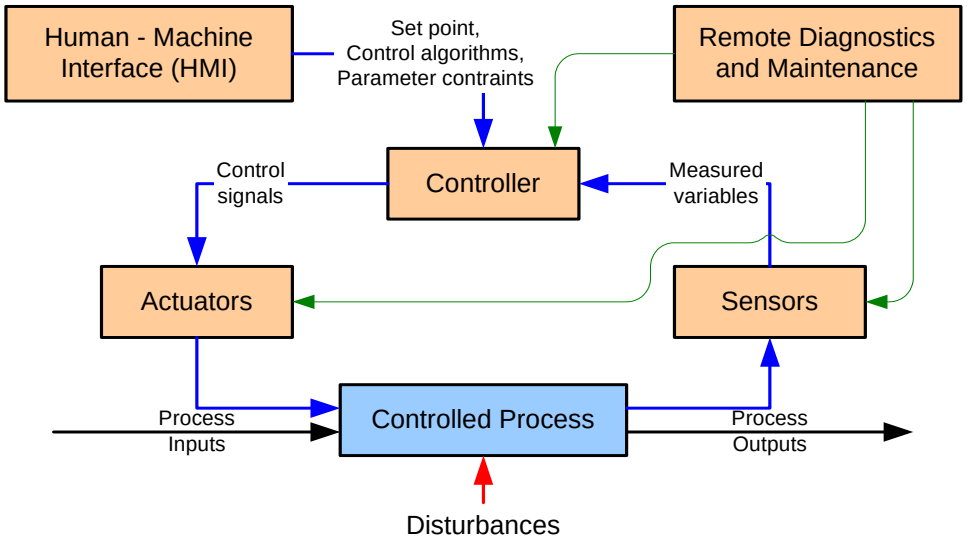

Figure 1. Generic Industrial Control System (ICS) (From Ref. SPP).

A SCADA system is an industrial measurement and control system consisting of a master station, one or more field data gathering and control units or remote terminal units (RTUs). They execute a collection of open and/or proprietary software and are used to monitor and control remotely located field data elements.

SCADA systems hardware can be broken down into the following five major categories; each with its own set of security associated risks. These layers are:

- Field level instrumentation and control devices
- Marshalling terminals and Remote Terminal Units (RTUs)
- Communications system
- Master station(s)
- Commercial data processing computer system [SCADA]

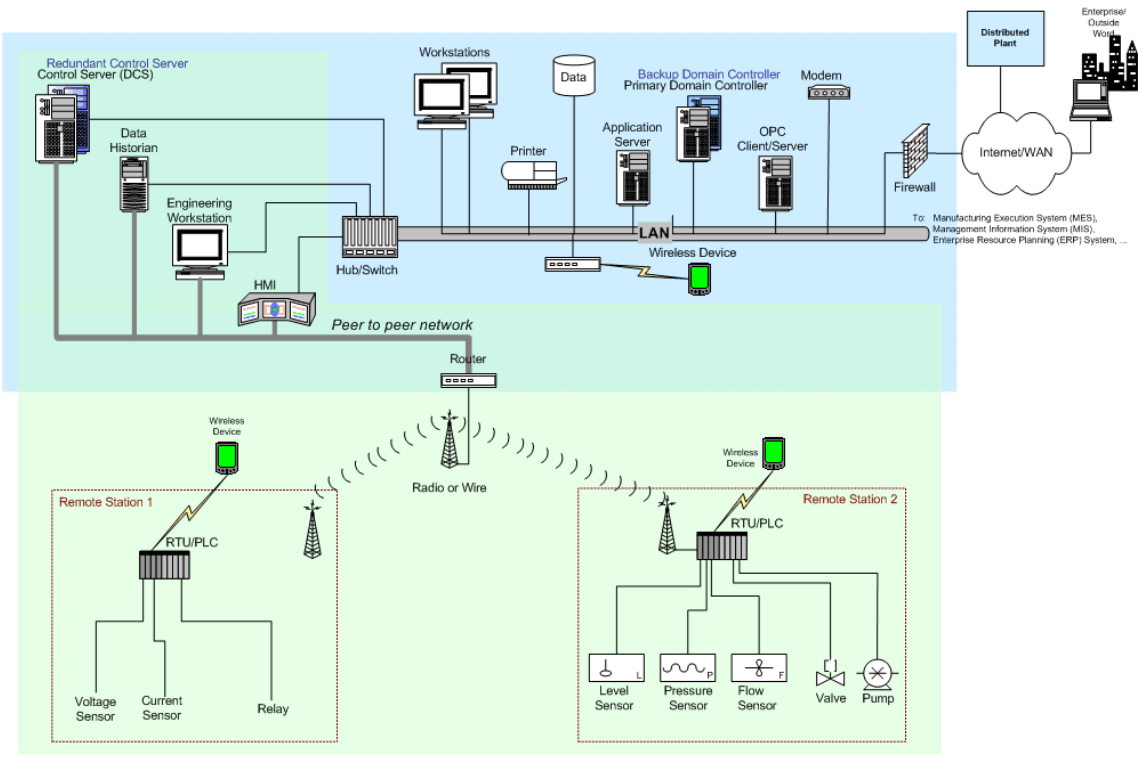

Figure 2. Generic SCADA system architecture. (From Ref. PCSRF)

The RTUs interface with remotely located field analog and digital sensors. The communications system provides a path for communication between the remote sites and the master station which may be in close proximity to each other or many miles apart. The master station gathers data from the RTUs and provides for an operator interface for the control of the remote sites and the display of information. [SCADA]

SCADA software can be either proprietary or open. Proprietary software is written by a company to only communicate with its hardware. Open software is becoming more attractive to consumers because it offers interoperability which enables users to mix components from different manufacturers within the same SCADA system. This severs the reliance on a single manufacturer. This open architecture also allows companies to replace specialized control devices and communications elements with general purpose computer equipment and communications technology. While very popular, this has contributed significantly to the cyber security threat. Of note, many SCADA master stations are implemented as Microsoft Windows applications. [DHS]

B. NETWORKS

SCADA system or process control system networks were initially designed to operate as isolated networks and therefore security design was neglected [MCDONNELL]. However, the economic realities have driven much of the SCADA system communications toward less expensive solutions based on the used of shared networks, such as the Internet or other IP networks. The trend to connect SCADA systems to corporate intranets for visibility and maintenance has created a backdoor for would-be cyber terrorists. Once highly proprietary, SCADA systems are currently being fielded using COTS technologies that rely on public Internet protocols for cost savings and management ease. [CW Hong Kong] A typical network architecture might look like the one in Figure 3 below.

Nearly all new sensor/actuator devices (generally called Intelligent Electronic Devices or IEDs) have a web interface that can be used for operating software upgrades and maintenance. The industries using SCADA systems have incorrectly assumed that the firewalls and the latest available network equipment provide adequate protection for the isolation of SCADA systems and corporate intranets from the Internet [OMNIV].

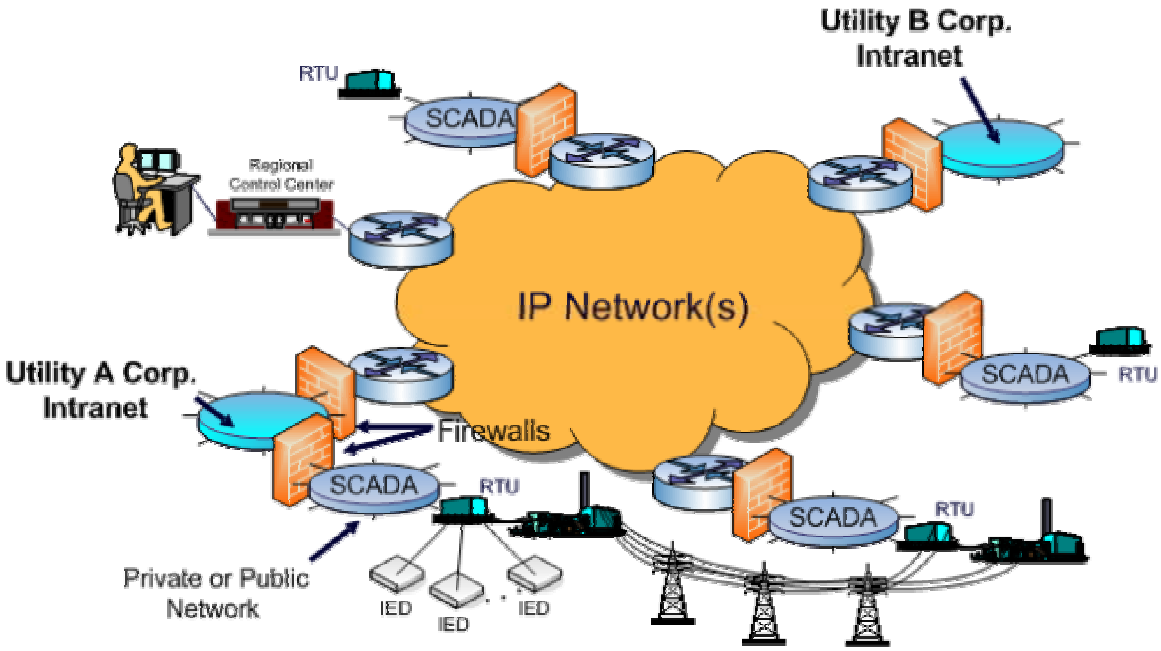

Figure 3. SCADA Communications Migration to IP Networks (From Ref. (OMNIV))

C. SCADA ATTACK EXAMPLES

A large number of security events and attacks, both in the past and more recently, have helped to increase general awareness of the security weaknesses of SCADA systems. The attacks listed below, with the exception of the last two are directly linked to the fact that there exists a path from the SCADA system network to the Internet. The list below is of noteworthy attacks. In reality, there were many more.

- On February 7, 2002, a vulnerability in a data transmission was discovered that was briefed to the President. The security flaw, according to the FBI, could have been exploited to bring down telephone networks and halt control information exchanged between ground and aircraft flight control systems. [WASHPT]
- SCADA devices are a global technology and it is understood that our enemies have access to and an in-depth understanding of the technology. Al Qaeda computers contained information about SCADA devices and how to hack them. After gleaning information from the contents of computers captured in Afghanistan and through prisoner interrogations, the Defense Intelligence Agency concluded that the Al Qaeda cyber threat is critical. [Blackout]
- North American Electric Reliability Council (NERC) files suggest that a cyber attack dry run took place in January 2003. The attack affected two unnamed utilities and their ability to execute bulk electric system control from their primary control centers for a few hours. [Blackout]
- The Maroochy Shire wastewater system had been leaking hundreds of thousands of gallons of wastewater sludge into parks, rivers, and the manicured grounds of a Hyatt Regency hotel for two months. On April 23, 2000, police stopped a car on the road to Deception Bay and found a stolen computer and radio transmitter. Using easily acquired technology, Vitek Boden had turned his vehicle into a command center for sewage treatment along Australia's Sunshine Coast. The arrest occurred while he was engaging in his 46th successful intrusion. [WASHPT]

- In 1998, a 12 year old broke into the computer system that runs Arizona's Roosevelt Dam. Federal authorities said he had complete command of the SCADA system controlling the dam's massive floodgates that hold back as much as 489 trillion gallons. That much water could theoretically cover the city of Phoenix, which is down river, to a height of five feet. [WASHPT]

- "Red Teams" of mock intruders from the Energy Department's four national laboratories have devised eight scenarios for SCADA attack on an electrical power grid. During exercises, these scenarios have been tested a total of eighteen times with complete success against large regional utilities companies. Systems that are almost identical run oil and gas utilities and many manufacturing plants. [WASHPT]

- During the KEMA Cyber Security Conference a presentation was given by an unidentified utility company of a 2 year-old targeted attack of the utility's real-time SCADA system. The critical elements of the attack were: 1.) The utility and the vendor each assumed the other was securing their part of the system - but neither took adequate steps to ensure protection. 2.) The vulnerable system that provided the path for penetration of the SCADA system was originally designed to have minimal use and exposure to the Internet - instead it actually had significant operating time. 3.) The attack resulted in significant financial impact to the utility even though they did not lose electric power and their customers were not physically affected. 4.) The utility lost use of its SCADA system for 2 weeks until the SCADA system could be completely reprogrammed and made a "trusted" system. 5.) The cost was 4 man-months of effort. 6.) As with others, the utility did not report the incident - there was no requirement to do so since no electric power was lost. [WEISS]

- A European utility reported at a recent CIGRE meeting that a virus attacked their Distribution SCADA system, and this resulted in partial

unavailability of the system functions. The utility reported they lost complete view of numerous distribution substations by the operators in the control center. Approximately 40 man-weeks (over a 4 calendar-week period) were required to mitigate the problem. This event was never reported. Additionally, the Chief Engineer for a very large Asian utility provided details of 3 cyber attacks on their critical electric facilities. [WEISS]

- In Bellingham, Washington in June 1999, a SCADA database modification was made that caused an extreme system slowdown of the system that controlled a gasoline pipeline. A pressure surge, which could have been handled if not for the system slowdown caused the pipe to rupture releasing 237K gallons of gasoline and killing three people. [NTSB]

- Based upon a report citing advances in Soviet technology through purchasing and copying U.S. technology, President Nixon placed restrictions on the export of computers and software to the Soviet Union. The K.G.B. responded to the restrictions by stealing or buying the technology through third parties. The C.I.A. found out about this in what French intelligence referred to as the Farewell dossier. Rather than deporting Soviet spies, Gus Weiss proposed a complex scheme to deliberately provide the Soviet with flawed technology. Through Farewell, the C.I.A. learned that one of their main priorities was to procure control system software to run their new gas pipeline. A dormant malicious program, commonly referred to as a "Trojan horse" was added to the software that ran the pumps, turbines, and valves of the pipeline (a SCADA system). The result of this was the largest non-nuclear explosion ever witnessed from space that happened in June 1982. This caused apprehensive Soviet scientists to delay or abandon all work that was based upon the software the K.G.B. had stolen for years. [SAFIRE]

The last two attack examples are particularly insidious since they were conducted by insiders.

D. CURRENT NATIONAL SCADA SECURITY POSTURE

President Clinton started the federal critical infrastructure protection (CIP) initiative in May 1998 with Presidential Decision Directive 63. That directive required agencies to protect the information systems that support the nation's infrastructure. However, reports from the General Accounting Office showed uneven progress in complying with PDD 63. Very few agencies met the 2003 deadline that it outlined. [PDD63] On December 17, 2003, President Bush signed a directive titled "Homeland Security Presidential Directive/Hspd-7" that replaces PDD 63. It mandates that by July 2004, the heads of all Federal departments and agencies shall develop and submit to the Director of the OMB plans for protecting the physical and cyber critical infrastructure and key resources that they own.[HSPD7]

The National Institute of Standards and Technology (NIST) Laboratory's mission is to conduct research that improves the nation's technology infrastructure. NIST also manages a Critical Infrastructure Grants program that funds research to provide solutions for the IT security problems of our nation's critical infrastructures. Through the NIST initiative on CIP, the Process Control Security Requirements Forum is supporting the development and dissemination of standards for process control and SCADA security. PCSRF is applying the ISO 15408 Common Criteria methodology to develop Protection Profiles for process control. Current work includes the creation of a Protection Profile for Industrial Control systems and the group is currently discussing the development of a SCADA protection profile [PCSRF].

The following is referenced from a statement given to Congress in March 2004 by Ben Wu, Deputy Under Secretary Technology Administration, U.S. Department of Commerce. In his testimony, Mr. Wu stated that the security of SCADA and building control systems could be enhanced. Delayed due to funding constraints, he is seeking an increase in FY 2005 funding (NIST funding increase from 10M to 16M) to help develop test procedures and guidelines for retrofitted cryptographic modules for SCADA systems

and to validate standards for SCADA and other ICS security. This aforementioned is necessary for NIST to fulfill one of its general responsibilities assigned under the Federal Information Security Management Act of 2002, which was to conduct research to identify information security vulnerabilities and to develop techniques to provide cost-effective security [TESTIM].

One of the program goals outlined by NIST relative to CIP is to increase the security of computer systems that control production and distribution in critical infrastructure industries. NIST plans to have this done by 2007. Working with the Process Control Security Requirements Forum (PCSRF), NIST is defining security requirement for products used in SCADA systems in hopes of influencing vendors to meet those requirements [NISTCIP].

E. CURRENT DOD SCADA IMPLEMENTATIONS

DoD is reliant upon SCADA systems as illustrated in the following examples.

United States Navy. SCADA systems are used on the Navy Mine Counter Measure ships to provide control and monitoring of various shipboard systems to include propulsion, lube oil, fuel oil, and firemain. [MCM] The Navy shipboard automation project undertaken jointly by Rockwell Automation and the Office of Naval Research seeks to implement Industrial Control Systems using commercial-off-the-shelf (COTS) hardware and intelligent software to manage ship engineering plants. [Rockwell] At the United States Navy shipyard at Pearl Harbor, Hawaii, the Navy awarded a contract to Transdyn for a Power Distribution/Substation monitoring and control SCADA system. [TRANSDYN]

United States Army. U.S. Army Corps of Engineers and ARINC Incorporated have teamed to provide advanced monitoring and control of electric power generation systems. ARINC SCADA systems use COTS software and hardware and open industry standards for low cost and high flexibility . [ARINC]

United States Air Force. Designated as a showcase facility, Edwards Air Force Base has an administration facility that uses a SCADA system to control the heating,

ventilation, and air-conditioning (HVAC) systems of numerous facilities. [DODENERGY]

All of the above either are connected to the Internet or have to capacity to be so connected. The secure operation of these systems is imperative.

F. DEPARTMENT OF THE NAVY'S CIP PROGRAM (DON CIP)

The DoN CIP program is an enterprise-wide partnership of organizational entities that are essential for DoN to achieve effective protection of critical infrastructures. Working closely with regional infrastructures in Naval concentration area, the DON CIP leverages efforts of DOD to develop integrated physical/cyber and on/off-base infrastructure protection strategies for physical and cyber components both on and off base. This is being done to enhance the protection of DOD/DON mission essential infrastructures. [DONCIP].

A key element of the DoN's CIP Program strategy is the Naval Integrated Vulnerability Assessment (NIVA) process. This process is used to identify and evaluate critical vulnerabilities and single points of failure by helping to protect mission critical cyber and physical mission essential infrastructures. The NIVA process is supported by four assessments pillars that cover the areas of Anti-Terrorism and Force Protection, Commercial Dependencies, Computer Network Defense (CND), and Consequence Management.

Anti-Terrorism and Force Protection addresses the vulnerability to a deliberate physical attack or the effects of an accident or a natural disaster on a critical infrastructure. The Commercial Dependencies portion of the NIVA process assesses the reliability and robustness of commercially supplied services (electricity, water, etc.) that are required to perform those mission essential functions necessary to execute the warfighting mission. The CND component examines the ability of an asset to withstand a cyber attack. The final pillar of the NIVA process, Consequence Management, tests the viability and integration of four plans that were deemed necessary should an attack against a mission critical asset occur. Theses four plans are: Continuity of Operations, Disaster Recovery, Response, and Reconstitution [CIPIMI].

The NIVA process also makes use of the CIP Event Cycle shown in the Figure 4 below. The six phases of the CIP cycle covers activities that could occur before during and after an event that could result in infrastructure destruction or disruption. As shown, the CIP Event Cycle is broadly broken up into two Modules. Module One constitutes activities that can take place prior to an event whereas Module Two contains the actions that the agency has already planned to take in response to an event.

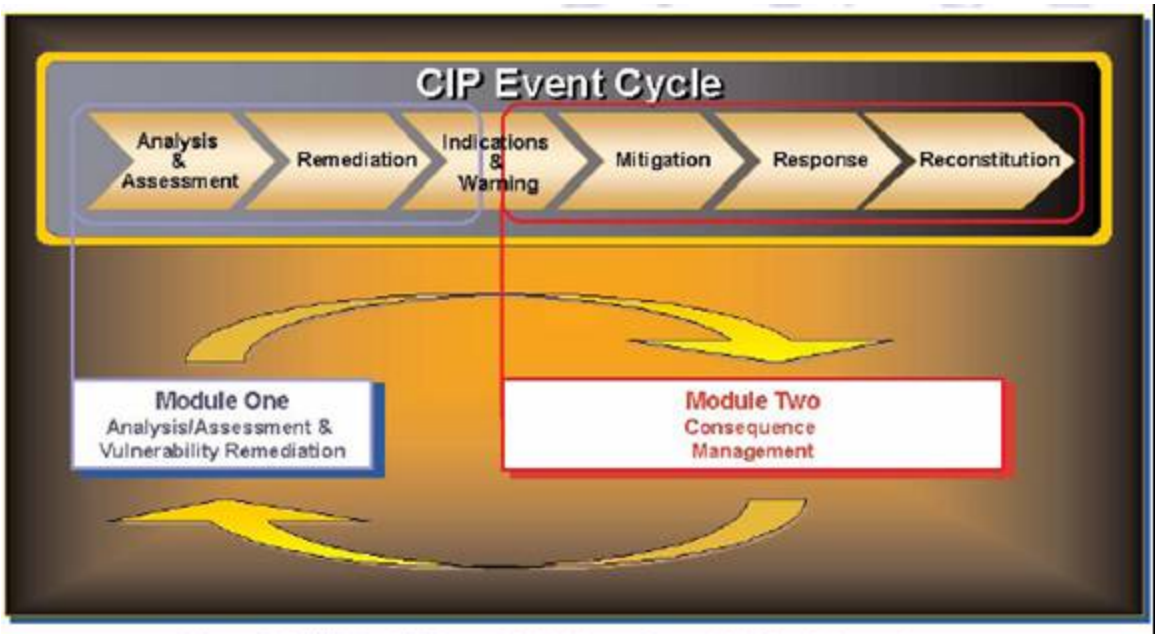

Figure 4. CIP Event Cycle. (From Ref. NIVA)

The Analysis/Assessment phase of Module One calls for the identification and development of a prioritized list of mission critical assets. This is followed by an assessment of those critical assets to find potential vulnerabilities and single points of failure that would disrupt the military's mission if they were exploited. The Vulnerability Remediation phase is next. This is the process of taking precautionary measures to improve the reliability, availability, and survivability of those assets identified during the Analysis/Assessment phase. Remediation normally occurs after vulnerabilities and single points of failure have been identified. [NIVA]

As stated earlier, the NIVA process is also concerned with Commercial Dependency assessment which seeks to identify critical dependencies on commercial

utilities. Like most other entities, the DoN is dependent on both organic assets i.e., a communications site and nonorganic assets such as the electric power and telecommunications utilities needed to support the asset. Electric power and telecommunications facilities make extensive use of SCADA systems. It is worth noting that the NIVA process does not seek to perform vulnerability assessments on SCADA assets belonging to nonorganic commercial entities.

G. DITSCAP PROGRAM

The Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) is the standardized approach designed to guide DoD agencies through the certification and accreditation (C & A) process. The C & A process exists to protect and secure entities that make up the Defense Information Infrastructure. There are four phases to the DITSCAP process. The phases are definition, verification, validation, and post-accreditation. During the definition phase, all system requirements and capabilities are documented to include mission, function, and interfaces. The resulting deliverable is a preliminary System Security Authorization Agreement (SSAA). In the verification phase, recommended changes to a system are performed and the resulting deliverable is a refined SSAA. The validation phase proceeds with a review of the SSAA. Vulnerability and penetration tests are also performed and the deliverable is a certification package containing the final SSAA and an approval or disapproval to operate. [DITSCAP]

Referring back to the Navy example of the SCADA system used on the Navy Mine Counter Measure ships it is expected that these systems would have been certified and accredited via the DITSCAP. A search for SSAAs of SCADA systems was conducted. My research has not produced a single SSAA, thus far, for DoN SCADA systems although such systems are widely used on Navy vessels. Points of contact in the Navy Information Assurance community have stated that the systems were considered closed-loop and therefore did not need to go through the C & A process. Industry trends and the quest of military members for ease of maintenance suggest that these systems will become more “open” or accessible and therefore this decision should be reconsidered.

The initial vulnerability assessment checklist produced by this study could be used in the C & A process as it would be implemented for SCADA systems.

H. SUMMARY

This chapter gave an overview of SCADA systems, what they are used for and where they are located. Examples of attacks on SCADA systems were presented. These illustrate how highly vulnerable SCADA systems are today. It also pointed out some of the SCADA system usage in the DoN/DoD, most importantly, their use aboard Navy vessels. It also introduced the NIVA process that the DoN uses to ascertain the vulnerabilities to its critical infrastructures that may could prevent the accomplishment of its mission. A short overview of the DITSCAP process and the possible application of this research to it was given as well.

THIS PAGE INTENTIONALLY LEFT BLANK

III. VULNERABILITY ASSESSMENTS

This section will give the reader background on vulnerability assessments by defining vulnerability assessment, discussing attack vectors, and providing some of the technical and procedural items to assess. Some threats and vulnerabilities of SCADA systems will also be presented.

A. VULNERABILITY ASSESSMENT

A vulnerability assessment is the systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation. [CIAO] In an assessment, the assessor should have the full cooperation of the organization being assessed. The organization should grant access to its facilities, provides network access, outlines detailed information about the network, etc. All parties acknowledge that the goal is to study security and identify improvements to secure the systems.

Vulnerability assessments provide a "snapshot in time" assessment of a system's or network's security posture As such, even when identified vulnerabilities are fixed or patched, future changes in configurations or permissions could open up entirely new holes. Additionally, new vulnerabilities in operating systems and applications crop up all the time. This means that, just because a particular system is patched and 'secure' today, the system may be deemed insecure when new vulnerabilities are discovered. Follow-up assessments will determine if old vulnerabilities have been fixed and can identify new ones that need to be addressed.[WINKLER]

B. ATTACK VECTORS

When putting together a 'checklist' for use when doing SCADA system vulnerability assessments, one should look at the three possible attack vectors. Refer to Figure 5. These are:

- Internet. The Internet poses a great danger because one has no control over it. Connecting your SCADA system network to the Internet for centralized operation and remote maintenance over public networks opens the door for tampering. While the trend is to allow such connections even down to the sensor/IED level, connecting components directly to the Internet allow for simplified invasion of your SCADA network.
- Corporate Network. The model for most control system networks is as shown in Figure 5 with no direct connection to the Internet. This model relies upon firewalls to protect it from cyber attack.
- Communications Path or Control System LAN (internal to the control system network. Also depicted in Figure 5 is the control system LAN as shown with the line around it. Legacy control system networks were totally separate from the corporate network and the Internet. That is usually not the case today with control system network. Also the movement within the process control arena toward open standards, mostly IP based, if an adversary can gain access to the control system LAN then the adversary has access every device on the network.

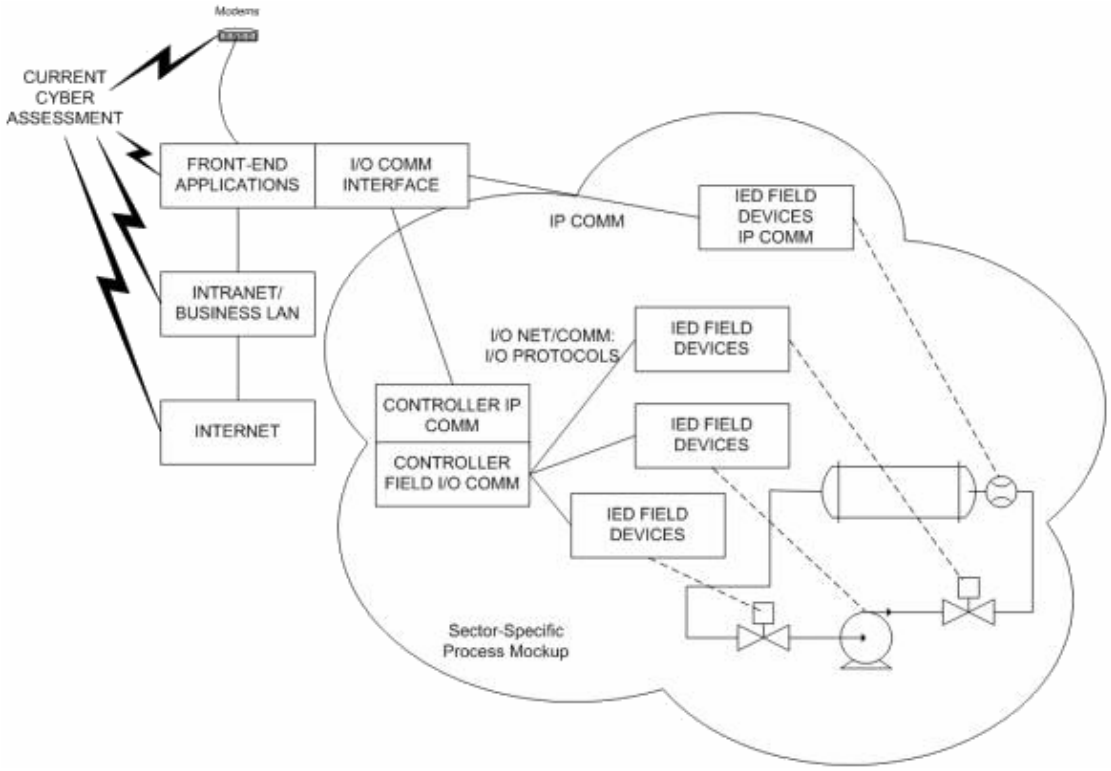

Figure 5. Current Cyber Assessment Model. (From Ref INEEL) Currently, the approach of cyber testing is to exploit IP data streams. IP includes the Internet, Intranet and control system LAN

Threats can be broadly broken down into two categories that need to be addressed: insider and outsider threats. Insiders include authorized users both inside and outside of the control system LAN and can include technicians, operators, and company staff. Threats from this group may or may not be intentional. The absence of security training and a good security policy should also be considered as an insider threat. In assessing the outsider threat, one should look at external communications paths, vendor support access, IP based communications utilizing private or public communications networks, web services, and operating system and hardware standardization. [NAGALA]. When using current low assurance commodity products, one can generally assume that the easier it is to manage the network, the easier it is for an adversary to attack it.

The Department of Energy, the Chemical Industry Data Exchange, and the Sandia National Laboratories have all published guidance or lessons learned from their

experience in assessing the cyber security of control systems. Each agency sited significant security issues with each SCADA system they assessed. Trends such as moving toward the full automation and networking of the systems and reliance on IP compounds the security issues. A thorough review of these documents provided the basis for the creation of the vulnerability assessment checklist.

C. TECHNICAL AND PROCEDURAL ITEMS TO ASSESS

1. System Data

Data is the fundamental element in any information architecture. Identification and classification of control system data into categories of similar sensitivity should be established. Without this distinction, it is impossible to determine where to apply security precautions to communications links, databases, etc. [INEEL]

A forensic flaw found in most control systems is the absence of capability to easily analyze data to determine if intrusions have occurred. Very few of the SCADA devices in today's market have the capability to examine control system traffic and determine if the traffic is legitimate or unauthorized. (Note: The capability does exist in some equipment that would allow you to determine if the traffic is the proper format and, to some extent, if the data is correct from a protocol standpoint. However, there are no devices that would allow you to analyze and determine if the traffic is correct for "that timeframe/conditions of the grid"). [PETERS]

2. Security Administration

SCADA systems should have security administration policies to aid in the implementation, operation, and maintenance of a secure system. Security procedures should include implementation guides, security plans, and security enforcement that include the use of auditing. Other important aspects of security administration are configuration management and security training of the staff and are necessary components of effective security administration. [INEEL]

3. Architecture

The architecture of the SCADA system should be reviewed to identify single points of failure. Whether or not the SCADA system is being leveraged to convey emergency signals such as security and fire alarms should be looked at as well since this can possibly introduce a backdoor into the system. [INEEL] Many control systems currently operate on low bandwidth communication paths. Dual use of these paths or unauthorized traffic on these paths (e.g., via worm, or non-prioritized download) may lead to loss of control of the affected devices. In some instances a loss of control may be as bad as compromise of the control device). [PETERS]

The architecture should avoid the use of inappropriate wireless communications. A lack of authentication in the 802.11 series of wireless communication protocols and an unfixable fundamental flaw that allows a Denial Of Service make the 802.11 series of protocols unsuitable for control system communications. A lack of authentication/security in other wireless communication mechanisms increases the risk of an adversary gaining access to the communication channel. The use of unsecured wireless communication for control networks should be avoided if possible. [PETERS]

4. Networks

Process control networks should be assessed to determine associated vulnerabilities. Legacy systems provide almost no inherent security and their network configuration warrants attention. Configuration passwords should be made as difficult to crack as possible. Wireless links are largely unprotected as they are usually broadcasts and of considerable length. Connections between the SCADA network and external networks can pose significant risk as well since they often consider the outside network as trusted. [INEEL]

Additionally poorly designed SCADA Control Networks that 1) fail to compartmentalize communication with the corporate network and other entities outside of the Control System; 2) fail to employ sufficient “defense in depth” mechanisms; 3)

fail to restrict “trusted access” to the control network; and 4) excessively rely on “security through obscurity” as a defensive mechanism. [PETERS]

The use of non-deterministic communications for command and control (in particular) Internet based SCADA constitutes another vulnerability. With non-deterministic communication you can not guarantee delivery and/or the path taken by the communications. This increases the risk of critical control system communications failure. The use of the Internet increases that risk of denial of service as it is a very adversary-friendly environment and attacks against other entities could greatly impact any control communications that uses this path or share resources that touch the Internet. Research has shown that a limited use of Virtual Private Networks (VPN) exists in control systems due to key management and other maintenance issues. One of the concerns is that an incorrectly configured VPN or one in which the operator forgets how to properly operate could cause a Denial of Service to the affected device. [PETERS]

5. Platforms

The computer platforms in SCADA networks fall broadly into two categories; proprietary or nonproprietary. Proprietary devices often have weak password control that can be defeated locally. Password access usually grants one complete control of the device. They often have a lack of defensive mechanisms to restrict administrative/maintenance access to control system components and have insufficient controls to protect against the installation of unauthorized software. [PETERS] Additionally, most devices offer the capability for remote access and configuration which greatly increases the need for physical protection. SCADA applications, interfaces, and databases are moving away from proprietary platforms to computers running Windows or UNIX operating systems. Default configuration of these platforms adds additional vulnerabilities. [INEEL]

Many control systems have not been developed to avoid standard Information Technology (IT) problems e.g., lack of boundary checks (i.e.: control signal or data input is outside reasonable numerical bounds) in control systems could lead to “buffer overflow” attacks against the control system software itself. This forms an additional

avenue of attack beyond the ones available due to the control system being run on a commercial operating system. SCADA communication protocols were never designed with security in mind and therefore the protocols themselves typically lack any form of authentication. If an adversary can gain access to the appropriate communication channel, the control system devices will accept any command given in that protocol. [PETERS]

Another problem is the lack of understanding of proper control system configurations including configurations of embedded system devices. This lack of understanding can contribute to the misconfiguration of operating parameters. Often delays occur in the implementation of software and firmware patches due to concerns of unintended effects on operations. An example of this is Service Pack 2 for Windows XP. This requires extensive testing of patches prior to implementation and may result in patches not being applied due to these "unintended" effects. [PETERS]

D. POSSIBLE THREATS AND VULNERABILITIES

1. Chemical Industry Data Exchange

The Chemical Industry Data Exchange published a list of some possible cyber security system vulnerabilities: [CIDX] Below is a partial list of items from that source that should be considered when performing a vulnerability assessment.

- Information technology product flaws requiring "fixes" after initial product installation
- Configuration and usage deficiencies of cyber security-technology products, such as retaining default system-supplied user ids and passwords
- Deficient cyber security processes (such as change management for IT or Process Control, and personnel processes such as identification revocation upon termination of system access)
- Lack of cyber security user training, for employees and contractors
- Lack of user awareness and adherence to sound security procedures (e.g., leaving your computer running unattended)

- Inadequately classified or protected electronic information that could be used to facilitate cyber security attacks
- Rogue access points, such as unmanaged modem access or Internet browser maintenance "back doors"
- Insufficient technology (for example, not installing a firewall)
- Use of remote access software (e.g., pcAnywhere®, Timbuktu®) programs that are typically used for access by experts within or outside the entity to support systems or operations. These applications can provide significant control and configuration access to an unauthorized individual.

One vendor web site even gives potential adversaries footprinting information by providing the model number of the equipment and the protocols used in a typical shipboard applications. [ROCK]

2. Internet Protocol (IP) Vulnerabilities

IP Networks, including the Internet, were designed to provide robust, ubiquitous any-to-any connectivity for the Wide Area Networks (WANs) used by the Nation's data network infrastructure. Such networks have four common architectural characteristics that make them unsuitable for SCADA system communications. IP Networks are:

- Connectionless – each packet contains sufficient information about the source and destination to route packets from any source to any destination without requiring a specific connection or route.
- Stateless – the control nodes in the network (routers) are not aware in a timely manner of the state of the network at any given time. The network will recover from events that change its state, but the time constants involved are orders of magnitude longer than the duration of those events.
- In-band Control – the signaling and control protocol traffic shares the same IP links as the bearer traffic. Users of the network have access to and can introduce these control packets as valid user traffic.

- Autonomous, distributed Control – Each control node (router) is independent (a peer) of all other nodes. No integrated, end-to-end control is possible [OMNIV].

3. 802.11 Vulnerabilities

Customers have been asking substation IED vendors to incorporate an 802.11 (Wi-Fi) interface into substation IEDs despite many studies reporting security problems [WIFI]. The Medium Access Control layer of the 802.11 protocol, in all its various releases, e.g.: 802.11a, 802.11b, 802.11g, is based on the exchange of request/response messages. Each request sent by a station in the network triggers a corresponding response on its counterpart. Wireless networks rely on an access point (AP) or a set of them as a central node through which every communication is routed. The management frames of the 802.11 protocol sent to an AP triggers an elaboration of request-response messages with consequent consumption of computational resources.

To scheme used to cause a denial of service is quite simple: each request message sent by a station must be responded with a response message sent by the AP. Thus, sending out a Probe Request frame to an AP triggers the transmission of a proper Probe Response frame which contains information about the network managed by the AP. Before an 802.11 client can continue communication with an AP, it must first send an Authentication request. Since, an 802.11 client can be authenticated to multiple APs it must also send an association request to determine which AP will be responsible for forwarding packets to the client. Authentication Requests and Association Requests cause corresponding responses from the AP. Probe Request, Authentication Request and Association Request flooding attacks can be executed by any malicious station in the area of a wireless network without being associated nor authenticated to the AP. [GIANLUI]

4. Attack Demonstration and Current Industry Trends

a. Attack Demonstration

At the KEMA Control System Cyber Security Workshop held from August 16-18, 2004 in Idaho Falls, ID, the Idaho National Engineering and Environmental Laboratory (INEEL) staff demonstrated two control system attack

scenarios. The first was an attack from a PC located locally by a person with cyber security, but not control system knowledge. The second attack utilized a recently identified system vulnerability to attack a typical substation SCADA system and was initiated remotely by Sandia National Laboratory (SNL) personnel from Albuquerque. The remote computer was connected to the local corporate LAN via a VPN connection. The attack was directed at a simulated substation SCADA system at INEEL (approximately 800 miles away).. The exploit was sent through the VPN connection from the corporate LAN to the SCADA LAN, and then through the firewall protecting the substation SCADA system. The attackers were able to perform the following functions:

- Open a breaker at the substation
- Open and close all breakers at the substation
- Change the SCADA Human Machine Interface breaker status representation on the operator's console display to indicate that a breaker was open while in reality it was not
- Open a breaker at the substation while completely hiding the actual status of the breaker from the operator's displays.

b. Industry Trends

Microsoft gave a presentation at the above mentioned conference that included discussion on security improvements with Windows XP Service Pack 2. These services include improved security in e-mail, Instant Messaging, and web services. When it was pointed out that good business practice would preclude the use of those services in control system applications, Microsoft said that the it was being pressed to include them by control system vendor customers. The customers even advocated adding services such as Real Player. The control system community of users and vendors needs to speak with one voice about the requirements for availability of these services in the control room environment in order to get the control system cyber security threat under

control. While some of the control system vendors are recommending that installing Service Pack 2 should be avoided, Microsoft expressed concern and disagreed with this position.

A review of web sites and conference exhibits show that many of the control system vendors are offering products with direct Internet connections to SCADA systems, RTUs, IEDs, transformers, etc. with no consideration given to the impacts on the cyber security of these systems and devices.

E. SUMMARY

This chapter examined some of the possible information assurance threats and vulnerabilities to a SCADA system. A definition of vulnerability assessment was given along with the background information that contributed to the development of the preliminary checklist.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. DEVELOPING AND VALIDATING A VULNERABILITY ASSESSMENT FOR SCADA SYSTEMS

In order to develop a preliminary vulnerability assessment, this study looked at current approaches, developed a checklist of items to consider, crafted a vulnerability assessment checklist to be used in a case study, and performed the case study to validate the checklist. These activities are detailed below. The section concludes with lessons learned and recommendations.

A. VULNERABILITY ASSESSMENT PROCEDURE

1. Methodology

The approach taken was that outlined for a risk assessment in the DoN CIP Self Assessment Tool and Reference Guide [DONCIP]. This guide includes provisions for identifying critical assets and performing vulnerability assessments. The guide provided a draft NIST self-assessment guide for Information Technology Systems that was designed to allow security managers and system administrators to audit their security policies and procedures.[NIST 800]

The NIST self-assessment guide utilizes an extensive questionnaire containing specific control objectives against which a system or group of interconnected systems can be tested and measured. It does not establish new security requirements. The control objectives are abstracted directly from long-standing requirements found in statute, policy, and guidance on security and privacy. The guide's questionnaire was an excellent starting point that provided most of the material needed to conduct the assessment once viewed from a control system context. This questionnaire is provided in Appendix A.

Questions from the NIST guide are separated into three major control areas: 1) management controls, 2) operational controls, and 3) technical controls. The guide uses the Federal Information Technology Security Assessment Framework (Framework) that identifies five levels of IT security program effectiveness five measures to determine whether the security control is being implemented:

- Level 1 – control objective documented in a security policy

- Level 2 – security controls documented as procedures
- Level 3 – security relevant procedures have been implemented
- Level 4 – security relevant procedures and security controls are tested and reviewed
- Level 5 – security relevant procedures and security controls are fully integrated into a comprehensive program.

For additional information on the Federal Information Technology Security Assessment Framework, refer to NIST SP 800-26 for details on what conditions have to be met in order to satisfy each of the levels.

B. VULNERABILITY ASSESSMENT OF AGENCY X

1. Initial Check List

An effective protection system for process control protects all of the critical functions of the system and their interfaces. The items listed below were considered in building the initial checklist but should not be deemed as all encompassing:

- Communications
    1. How are the remote acquisitioning units communicating to the master station?
    2. Are the communication channels protected, for example with encryption, and is redundancy built into the overall SCADA system?
    3. What protocols are being used and what are their vulnerabilities?
- Commercial hardware and software and firmware
    1. What operating system is the hardware running?
    2. Has the operating system been hardened and unnecessary services disabled?
    3. Is there a password policy and is it being enforced?
- Application software

1. Isconfiguration control implemented for application software?
2. Is the application software from a trusted source and is it adequately tested?

- Parameter data
  1. Are key parameter data files set to “Read only?”
  2. Is authentication required to write to data files?
- Support infrastructure
  1. Does the system have backup power?
  2. What are the environmental controls?

If one of the above listed functions is not protected, the adversary could exploit it to use the process control system to cause an undesired event. If not properly safeguarded, the adversary would not require physical access to trigger the event. [NIJ]

A determination needs to be made as to access to the process control system and should include:

- List of authorized users
- Means and routes of access to the system
- Protection features of the system and their utilization
  1. Passwords
  2. Physical access control

The presence of the items listed below represents some of the things to look for when conducting a vulnerability assessment since they can improve the protection of process control networks are:

- Protected and strong passwords and password policies

1. Is there a password policy and is it being enforced?
2. Do all users have administrative privileges?
3. Are passwords shared?
4. Do the passwords expire, etc?

- Firewalls
  1. Are required firewalls in place; if not why not?
  2. Is there a firewall policy?
  3. How are the firewalls configured
  4. How are they maintained, etc.?
- Configuration Control
  1. Is configuration management practiced?
  2. Is there a formal procedure for configuration management?
- Is virus protection installed and up-to-date?
- Are encryption and authentication appropriate?
- In terms of redundant communication, are there any single points of failure in the system?
- Is the process control network isolated from the external network?
- Are process control sensors routed to alarm control center?

C. LESSONS LEARNED FROM CASE STUDY

When conducting the assessment of Agency X's SCADA system, it was noted that not enough emphasis is placed on physical security since the technical controls normally employed in traditional IT systems are often not used. Initially, the NIST questionnaire was used in conjunction with some additional references for firewall, router, remote access, and wireless network policies. It was quickly determined that the NIST questionnaire did not going to be a perfect fit the for the SCADA system

vulnerability assessment checklist mainly due to what the ISA refers to as special considerations. The NIST questionnaire did, however, with slight modification adequately address the common vulnerabilities found in SCADA systems as outlined by Sandia, ISA, CIDX, INEEL, and NERC.

SCADA systems are complex and are all slightly different. Not realizing these differences caused the assessor to make some assumptions that were incorrect. The NIST questionnaire assumes the presence of a security policy and so did the assessor. No written policies or even network diagrams were in place. The assessor should have allowed more time for Agency X to review the questionnaire prior to the assessment and capture on paper some of the undocumented policies that it was following. That could have provided a more accurate picture of their security posture.

D. DEVELOPMENT OF THE DON PRELIMINARY SCADA VA CHECKLIST

NIST SP 800-26 provided an excellent framework for conducting a vulnerability assessment because of its comprehensiveness. To apply the NIST checklist to a DoN SCADA vulnerability assessment, it was necessary to remove some of the checklist items and redefine some others as they relate to SCADA. Appendix B captures lessons learned from the case study and extensive research. Items from the NIST checklist have been removed, modified, or recommended for further consideration. The rationales for the changes from the NIST checklist that have been incorporated in Appendix B are discussed below.

Since oftentimes many of the traditional IT security mechanisms are ignored in the SCADA environment, it may be necessary to place emphasis on Section 7 of the NIST checklist, Physical and Environmental Protection during an assessment. .

It is recommended that the following items be considered for further study and refinement. However, until then, they could be deleted from the NIST checklist

1. NIST currently has a proposal to write a SCADA protection profile that will identify security requirements for SCADA systems. This research located no other

guidelines or policy for SCADA security requirements or controls. Until a set of security requirements or controls is identified, Section 3, Life Cycle, items in section 3.1 could be removed. When requirements are complete, Section 3.1 items will have more relevance.

2. Section 11, Data Integrity, until a requirement is levied on SCADA system manufacturers to provide a method for ascertaining data integrity, it is useless to assess sub-items in section 11.2. The most that one can expect in today's SCADA systems is a check to ensure that the traffic is in the proper format according to the protocol and not whether it is legitimate. [PETERS] Recommend leaving item 11.2 in the checklist and deleting the sub-items.

3. Section 16.3 can be removed since public access to the SCADA system is not allowed.

The following are items that needed some redefining.

1. Section 10, Hardware and System Software Maintenance, item 10.3.2. This item asks if software patches are promptly installed. SCADA environments normally do not abide by this rule. Patches applied to SCADA systems must be tested thoroughly since these systems often run continuously. They can ill afford the unintended effects that adding a patch may have on system operation and are often not applied at all. Determining if there is a policy in place for the testing of software and firmware patches and how well they follow the policy is the most that can be expected from SCADA system owners. [ISA]

2. Sections 15 – 17 fall broadly under the NIST heading of Technical Controls. Today's SCADA systems would fail when assessed against the criteria outlined in these three sections. ISA-TR99.00.02-2004 has devoted section 6.5 to "Special Considerations for Manufacturing and Control Systems. It outlines some of the critical operational differences between those systems and traditional IT systems that mandate how some security measures should be applied. [ISA]

3. Section 15, Identification and Authentication. According to the ISA, certain emergency actions should not be hampered by passwords. This violates both

critical elements of section 15 of the NIST checklist. Passwords do have their place in a SCADA environment, i.e., access to perform system configuration, and their use should not be totally discounted, as was observed in this case study. It is suggested that the section is left as is and tailored for the specific SCADA system application.

4. Section 16, Logical Access Controls. At the core of logical access control mechanisms is the ability to identify and authenticate users. The way passwords are utilized and not utilized in the SCADA environment hampers this effort. This section should be left in since agencies such as NIST recognize the need for access control and are working to build a protection profile for a SCADA that will have mechanisms in place to address this issue. Item 16.2.11 discusses firewalls and their compliance with firewall policy and rules. Refer to the Navy Marine Corps Unclassified Trusted Network Protect Policy, if applicable, or to the NIST SP 800-41, Guidelines on Firewalls and Firewall Policy, to ensure compliance with this objective. Many objectives contained in section 16 can be met today. [PETERS]

5. Section 17, Audit Trail, present most of the same issues noted with Sections 15 and 16. Poor password policy precludes an effective auditing program. Again, however, in cases where possible, auditing can be effective if practiced.

E. SUMMARY

This chapter examined the possible information assurance threats and vulnerabilities to a SCADA system. There are indicators to look for when doing an assessment that, if in place, enhances the systems security This chapter discussed the methodology employed to perform the assessment of the SCADA system. It also gave some solutions to mitigate some of the vulnerabilities found during the assessment. From the extensive research and lessons learned from conducting the case study of Agency X, a preliminary vulnerability assessment checklist for SCADA systems for use by the DoN was developed.

THIS PAGE INTENTIONALLY LEFT BLANK

V. RECOMMENDATIONS AND CONCLUSIONS

A. RECOMMENDATIONS

This thesis sought to produce a preliminary vulnerability checklist for use by the DoN in assessing its SCADA systems. While it is noted that all SCADA systems are likely to be in a different configuration, the major components and vulnerabilities remain the same. The following are some recommendations and conclusions found during the course of this study.

1. Expand the SCADA Laboratory

Initially, the validation of my research was going to be performed in the SCADA laboratory. Time and roadblocks prevented the completion of the SCADA laboratory. The addition of more components to the laboratory will more accurately simulate a real process control network. Then it will be useful for vulnerability assessment exercises. Additionally, real penetration testing can be conducted in the laboratory since it won't be a part of a live network.

2. Incorporate SCADA Systems into the DITSCAP Process

All research pointed to the fact that, while recognized as computer-based IT systems, SCADA systems were not incorporated into the DITSCAP process. Industry trends are moving toward the incorporation of more open standards and the reliance upon the Internet for SCADA system maintenance and reporting. SCADA components such as RTUs and IEDs are being designed and built today with capability to connect to the Internet. These connection points must be secured even if not actively connected to prevent someone with access from maliciously or accidentally establishing a connection. Although it may not be part of the network diagram, if the connection point is there, the possibility for its use exists and should therefore be acknowledged and carefully monitored through the use of a structured C & A process such as the DITSCAP.

3. Future Work

During this research, an interesting new technology was identified that warrants some additional attention. The technology claims that it can solve the problems that exist in today's IP networks, without replacing them, and provide SCADA system communication with reliable, deterministic performance by the network. The Emergency Telecommunications Services (ETS) has a draft technical report out that lists its requirements for network reliability and the technology in Figure 6 claims to meet them all [ETS]. The requirements set forth by ETS in the technical report are that the communication be:

- Connection-oriented – each communication of critical data happens in a registered session over a virtual circuit, i.e., for the duration of a given session, traffic is sent over a pre-planned route or routes with characteristics known by a stateful management process;
- Stateful – network management uses an automated process to gather and maintain link characteristics used to plan virtual circuit routes with sufficient regularity to control and respond to events of a given duration. For example, for a voice call, events of interest have durations on the order of tens of milliseconds (10^{-2} sec). State information granularity must, therefore, be of the order of milliseconds (10^{-3} sec) or less.
- Controlled Out-of-band – the network must prevent user access to signaling and control traffic. This problem occurred in the public telephone system some decades ago and was solved by separating the control traffic from the voice traffic. A separate control network was overlaid onto the voice network to which users had no ready access. Although the other architectural traits have an impact on security, this characteristic is critical to reducing the vulnerability of IP Networks.
- Coherent, distributed Control – traffic over IP Networks is usually hauled by more than one Carrier. In order to have end-to-end control of the traffic, the control network needs the same ubiquitous coverage. This control should be

physically distributed to prevent having a single point of failure, but coherency is required to provide an end-to-end stateful view of the overall network. This facet also has significant impact on network vulnerability, especially in certain distributed attack scenarios.

This architecture comprises a so-called “Cognitive” Network that provides:

- Bandwidth management and guaranteed network performance, end to end;
- A means to monitor usage patterns to detect and counter attacks;
- A means to monitor and enforce communications Service Level Agreements;
- Superior privacy and network security;
- Significantly lower operating expenses with modest capital investment; and
- A backward-compatible, yet future-proof, solution to the fundamental problems of IP Networks.

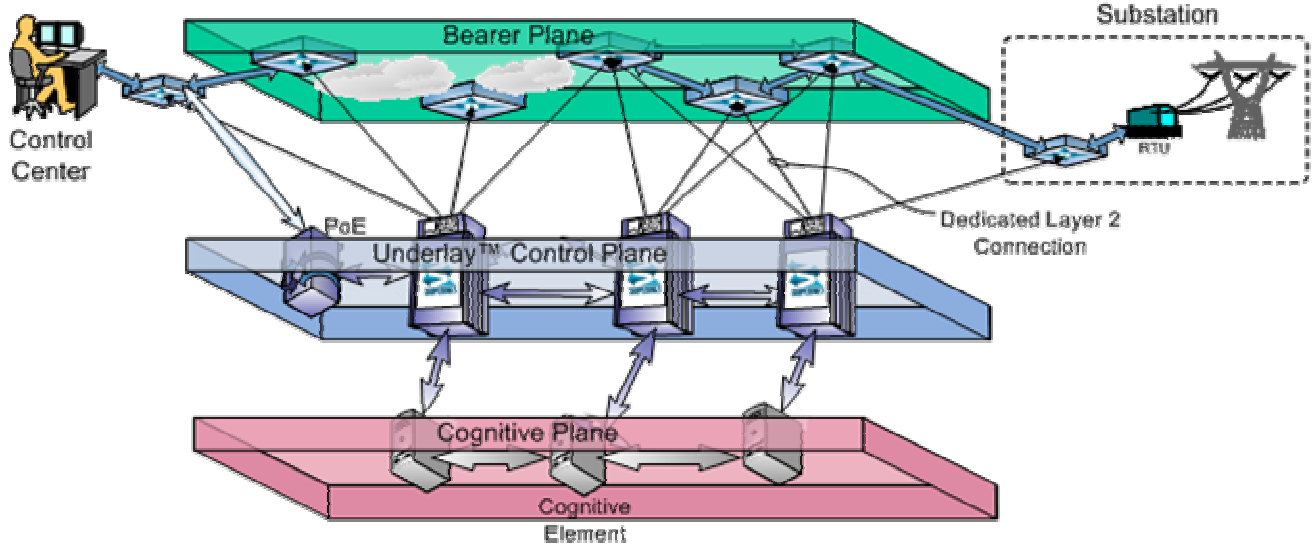

Figure 6. Simplified Cognitive Network Architecture (From Ref. OMNIV)

Research to ascertain its merit in securing SCADA communications from cyber attacks would be of benefit since the technology claims to be impervious to DOS, DDOS, masquerade, man-in-the-middle, and firewall attacks.

B. CONCLUSION

This thesis set out to produce a preliminary vulnerability checklist and lay the foundation for the creation of a more comprehensive checklist for vulnerability assessments of DoN SCADA systems to be used by DoN Assessment teams. A checklist was created and validated in a representative commercial dependency environment representative of what the DoN uses. More work needs to be done in encouraging commercial entities to treat seriously the threat posed by cyber attacks to process control networks. Moreover, the DoN also needs to examine its own process control networks in order to ascertain and mitigate that threat as well.

There exists a large chasm between the administration of corporate networks and SCADA system networks that needs to be bridged. For example, simple industry best practices such as password security are ignored in favor of trust for fear of self-inflicted denial of service attacks. There is also a need for a closer relationship between the corporate IT security personnel and the process control network administrators. Corporate IP security personnel have a better appreciation for cyber security since they have been concerned with it for at much greater period of time.

APPENDIX A. NIST SP 800-26 SELF-ASSESSMENT QUESTIONNAIRE

System Name, Title, and Unique Identifier: _____

Major Application _____ or General Support System _____

NAME OF ASSESSORS:

_____

_____

_____

Date of Evaluation: _____

List of Connected Systems:

Name of System	Are boundary controls effective?	Planned action if not effective
1.		
2.		
3.		

Criticality of System	Category of Sensitivity High, Medium, or Low
Confidentiality	
Integrity	
Availability	

Purpose and Objective of Assessment: _____

_____

_____

MANAGEMENT CONTROLS

Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management.

1. Risk Management

Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Risk Management *OMB Circular A-130, III*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
1.1 Critical Element: Is risk periodically assessed?								
1.1.1 Is the current system configuration documented, including links to other systems? *NIST SP 800-18*								
1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change? *FISCAM SP-1*								
1.1.3 Has data sensitivity and integrity of the data been considered? *FISCAM SP-1*								
1.1.4 Have threat sources, both natural and manmade, been identified? *FISCAM SP-1*								
1.1.5 Has a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources been developed and maintained current? *NIST SP 800-30*[1]								

1 Draft NIST Special Publication 800-30, "Risk Management Guidance" dated June 2001.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
1.1.6 Has an analysis been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities? *NIST SP 800-30*								
1.2. Critical Element: Do program officials understand the risk to systems under their control and determine the acceptable level of risk?								
1.2.1 Are final risk determinations and related management approvals documented and maintained on file? *FISCAM SP-1*								
1.2.2 Has a mission/business impact analysis been conducted? *NIST SP 800-30*								
1.2.3 Have additional controls been identified to sufficiently mitigate identified risks? *NIST SP 800-30*								

NOTES:

2. REVIEW OF SECURITY CONTROLS

Routine evaluations and response to identified vulnerabilities are important elements of managing the risk of a system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Review of Security Controls *OMB Circular A-130, III FISCAM SP-5 NIST SP 800-18*								
2.1. Critical Element: **Have the security controls of the system and interconnected systems been reviewed?**								
2.1 1 Has the system and all network boundaries been subjected to periodic reviews? *FISCAM SP-5.1*								
2.1.2 Has an independent review been performed when a significant change occurred? *OMB Circular A-130, III FISCAM SP-5.1 NIST SP 800-*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
18								
2.1.3 Are routine self-assessments conducted ? *NIST SP 800-18*								
2.1.4 Are tests and examinations of key controls routinely made, i.e., network scans, analyses of router and switch settings, penetration testing? *OMB Circular A-130, 8B3* *NIST SP 800-18*								
2.1.5 Are security alerts and security incidents analyzed and remedial actions taken? *FISCAM SP 3-4* *NIST SP 800-18*								
2.2. Critical Element: Does management ensure that corrective actions are effectively implemented?								
2.2.1 Is there an effective and timely process for reporting significant weakness and ensuring effective								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
remedial action? *FISCAM SP 5-1 and 5.2 NIST SP 800-18*								

NOTES:

3. LIFE CYCLE

Like other aspects of an IT system, security is best managed if planned for throughout the IT system life cycle. There are many models for the IT system life cycle but most contain five basic phases: initiation, development/acquisition, implementation, operation, and disposal. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Life Cycle *OMB Circular A-130, III* *FISCAM CC-1.1*								
3.1. Critical Element: **Has a system development life cycle methodology been developed?**								
Initiation Phase								
3.1.1 Is the sensitivity of the system determined? *OMB Circular A-130, III* *FISCAM AC-1.1 & 1.2* *NIST SP 800-18*								
3.1.2 Does the business case document the resources required for adequately securing the system? *Clinger-Cohen*								
3.1.3 Does the Investment Review Board ensure any investment request includes the security resources needed? *Clinger-Cohen*								
3.1.4 Are authorizations for software modifications documented and maintained? *FISCAM CC –1.2*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.1.5 Does the budget request include the security resources required for the system? *GISRA*								
Development/Acquisition Phase								
3.1.6 During the system design, are security requirements identified? *NIST SP 800-18*								
3.1.7 Was an initial risk assessment performed to determine security requirements? *NIST SP 800-30*								
3.1.8 Is there a written agreement with program officials on the security controls employed and residual risk? *NIST SP 800-18*								
3.1.9 Are security controls consistent with and an integral part of the IT architecture of the agency? *OMB Circular A-130, 8B3*								
3.1.10 Are the appropriate security controls with associated evaluation and test procedures developed before the procurement action? *NIST SP 800-18*								
3.1.11 Do the solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.1.12 Do the requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented? *NIST SP 800-18*								
Implementation Phase								
3.2. Critical Element: Are changes controlled as programs progress through testing to final approval?								
3.2.1 Are design reviews and system tests run prior to placing the system in production? *FISCAM CC-2.1* *NIST SP 800-18*								
3.2.2 Are the test results documented? *FISCAM CC-2.1* *NIST SP 800-18*								
3.2.3 Is certification testing of security controls conducted and documented? *NIST SP 800-18*								
3.2.4 If security controls were added since development, has the system documentation been modified to include them? *NIST SP 800-18*								
3.2.5 If security controls were added since development, have the security controls been tested and the system recertified? *FISCAM CC-2.1* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.2.6 Has the application undergone a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards? *NIST SP 800-18*								
3.2.7 Does the system have written authorization to operate either on an interim basis with planned corrective action or full authorization? *NIST SP 800-18*								
Operation/Maintenance Phase								
3.2.8 Has a system security plan been developed and approved? *OMB Circular A-130, III* *FISCAM SP 2-1* *NIST SP 800-18*								
3.2.9 If the system connects to other systems, have controls been established and disseminated to the owners of the interconnected systems? *NIST SP 800-18*								
3.2.10 Is the system security plan kept current? *OMB Circular A-130, III* *FISCAM SP 2-1* *NIST SP 800-18*								
Disposal Phase								
3.2.11 Are official electronic records properly disposed/archived? NIST SP 800-18								
3.2.12 Is information or media purged, overwritten, degaussed, or destroyed when disposed or used elsewhere? *FISCAM AC-3.4* *NIST SP 800-18*								
3.2.13 Is a record kept of who implemented the								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
disposal actions and verified that the information or media was sanitized? *NIST SP 800-18*								

NOTES:

4. AUTHORIZE PROCESSING (CERTIFICATION & ACCREDITATION)

Authorize processing (Note: Some agencies refer to this process as certification and accreditation) provides a form of assurance of the security of the system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Authorize Processing (Certification & Accreditation) *OMB Circular A-130, III FIPS 102*								
4.1. Critical Element: Has the system been certified/recertified and authorized to process (accredited)?								
4.1.1 Has a technical and/or security evaluation been completed or conducted when a significant change occurred? *NIST SP 800-18*								
4.1.2 Has a risk assessment been conducted when a significant change occurred? *NIST SP 800-18*								
4.1.3 Have Rules of Behavior been established and signed by users? *NIST SP 800-18*								
4.1.4 Has a contingency plan been developed and tested? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
4.1.5 Has a system security plan been developed, updated, and reviewed? *NIST SP 800-18*								
4.1.6 Are in-place controls operating as intended? *NIST SP 800-18*								
4.1.7 Are the planned and in-place controls consistent with the identified risks and the system and data sensitivity? *NIST SP 800-18*								
4.1.8 Has management authorized interconnections to all systems (including systems owned and operated by another program, agency, organization or contractor)? *NIST 800-18*								
4.2. Critical Element: Is the system operating on an interim authority to process in accordance with specified agency procedures?								
4.2.1 Has management initiated prompt action to correct deficiencies? *NIST SP 800-18*								

NOTES:

5. SYSTEM SECURITY PLAN

System security plans provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The plan delineates responsibilities and expected behavior of all individuals who access the system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
System security plan *OMB Circular A-130, III NIST SP 800-18 FISCAM SP-2.1*								
5.1. Critical Element: Is a system security plan documented for the system and all interconnected systems if the boundary controls are ineffective?								
5.1.1 Is the system security plan approved by key affected parties and management? *FISCAM SP-2.1 NIST SP 800-18*								
5.1.2 Does the plan contain the topics prescribed in NIST Special Publication 800-18? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
5.1.3 Is a summary of the plan incorporated into the strategic IRM plan? *OMB Circular A-130, III* *NIST SP 800-18*								
5.2. Critical Element: Is the plan kept current?								
5.2.1 Is the plan reviewed periodically and adjusted to reflect current conditions and risks? *FISCAM SP-2.1* *NIST SP 800-18*								

NOTES:

OPERATIONAL CONTROLS

The operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls.

6. PERSONNEL SECURITY

Many important issues in computer security involve human users, designers, implementers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives	**L.1** Policy	**L.2** Procedures	**L.3** Implemented	**L.4** Tested	**L.5** Integrated	**Risk Based Decision Made**	**Comments**	**Initials**
Personnel Security *OMB Circular A-130, III*								
6.1. Critical Element: Are duties separated to ensure least privilege and individual accountability?								
6.1.1 Are all positions reviewed for sensitivity level? *FISCAM SD-1.2 NIST SP 800-18*								
6.1.2 Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties? *FISCAM SD-1.2*								

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
6.1.3 Are sensitive functions divided among different individuals? *OMB Circular A-130, III FISCAM SD-1 NIST SP 800-18*								
6.1.4 Are distinct systems support functions performed by different individuals? *FISCAM SD-1.1*								
6.1.5 Are mechanisms in place for holding users responsible for their actions? *OMB Circular A-130, III FISCAM SD-2 & 3.2*								
6.1.6 Are regularly scheduled vacations and periodic job/shift rotations required? *FISCAM SD-1.1 FISCAM SP-4.1*								
6.1.7 Are hiring, transfer, and termination procedures established? *FISCAM SP-4.1 NIST SP 800-18*								
6.1.8 Is there a process for requesting, establishing, issuing, and closing user accounts? *FISCAM SP-4.1*								

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
NIST 800-18								
6.2. Critical Element: **Is appropriate background screening for assigned positions completed prior to granting access?**								
6.2.1 Are individuals who are authorized to bypass significant technical and operational controls screened prior to access and periodically thereafter? *OMB Circular A-130, III FISCAM SP-4.1*								
6.2.2 Are confidentiality or security agreements required for employees assigned to work with sensitive information? *FISCAM SP-4.1*								
6.2.3 When controls cannot adequately protect the information, are individuals screened prior to access? *OMB Circular A-130, III*								
6.2.4 Are there conditions for allowing system access prior to								

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
completion of screening? *FISCAM AC-2.2 NIST SP 800-18*								

NOTES:

7. PHYSICAL AND ENVIRONMENTAL PROTECTION

Physical security and environmental security are the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Physical and Environmental Protection								
Physical Access Control								
7.1. Critical Element: Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?								
7.1.1 Is access to facilities controlled through the use of guards, identification badges, or entry devices such as key cards or biometrics? *FISCAM AC-3 NIST SP 800-18*								
7.1.2 Does management regularly review the list of persons with physical access								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
to sensitive facilities? *FISCAM AC-3.1*								
7.1.3 Are deposits and withdrawals of tapes and other storage media from the library authorized and logged? *FISCAM AC-3.1*								
7.1.4 Are keys or other access devices needed to enter the computer room and tape/media library? *FISCAM AC-3.1*								
7.1.5 Are unused keys or other entry devices secured? *FISCAM AC-3.1*								
7.1.6 Do emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter after fire drills, etc? *FISCAM AC-3.1*								
7.1.7 Are visitors to sensitive areas signed in and escorted? *FISCAM AC-3.1*								
7.1.8 Are entry codes changed periodically? *FISCAM AC-3.1*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
7.1.9 Are physical accesses monitored through audit trails and apparent security violations investigated and remedial action taken? *FISCAM AC-4*								
7.1.10 Is suspicious access activity investigated and appropriate action taken? *FISCAM AC-4.3*								
7.1.11 Are visitors, contractors and maintenance personnel authenticated through the use of preplanned appointments and identification checks? *FISCAM AC-3.1*								
Fire Safety Factors								
7.1.12 Are appropriate fire suppression and prevention devices installed and working? *FISCAM SC-2.2* *NIST SP 800-18*								
7.1.13 Are fire ignition sources, such as failures of electronic devices								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
or wiring, improper storage materials, and the possibility of arson, reviewed periodically? *NIST SP 800-18*								
Supporting Utilities								
7.1.14 Are heating and air-conditioning systems regularly maintained? *NIST SP 800-18*								
7.1.15 Is there a redundant air-cooling system? *FISCAM SC-2.2*								
7.1.16 Are electric power distribution, heating plants, water, sewage, and other utilities periodically reviewed for risk of failure? *FISCAM SC-2.2* *NIST SP 800-18*								
7.1.17 Are building plumbing lines known and do not endanger system? *FISCAM SC-2.2* *NIST SP 800-18*								
7.1.18 Has an uninterruptible power supply or backup								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
generator been provided? *FISCAM SC-2.2*								
7.1.19 Have controls been implemented to mitigate other disasters, such as floods, earthquakes, etc.? *FISCAM SC-2.2*								
Interception of Data								
7.2. Critical Element: Is data protected from interception?								
7.2.1 Are computer monitors located to eliminate viewing by unauthorized persons? *NIST SP 800-18*								
7.2.2 Is physical access to data transmission lines controlled? *NIST SP 800-18*								
Mobile and Portable Systems								
7.3. Critical Element: Are mobile and portable systems protected?								
7.3.1 Are sensitive data files encrypted on all portable systems?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
NIST SP 800-14								
7.3.2 Are portable systems stored securely? *NIST SP 800-14*								

NOTES:

8. PRODUCTION, INPUT/OUTPUT CONTROLS

There are many aspects to supporting IT operations. Topics range from a user help desk to procedures for storing, handling and destroying media. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Production, Input/Output Controls								
8.1. Critical Element: Is there user support?								
8.1.1 Is there a help desk or group that offers advice? *NIST SP 800-18*								
8.2. Critical Element: Are there media controls?								
8.2.1 Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information? *NIST SP 800-18*								
8.2.2 Are there processes for ensuring that only authorized users pick up, receive, or deliver input and output information and media?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
NIST SP 800-18								
8.2.3 Are audit trails used for receipt of sensitive inputs/outputs? *NIST SP 800-18*								
8.2.4 Are controls in place for transporting or mailing media or printed output? *NIST SP 800-18*								
8.2.5 Is there internal/external labeling for sensitivity? *NIST SP 800-18*								
8.2.6 Is there external labeling with special handling instructions? *NIST SP 800-18*								
8.2.7 Are audit trails kept for inventory management? *NIST SP 800-18*								
8.2.8 Is media sanitized for reuse? *FISCAM AC-3.4* *NIST SP 800-18*								
8.2.9 Is damaged media stored and /or								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
destroyed? *NIST SP 800-18*								
8.2.10 Is hardcopy media shredded or destroyed when no longer needed? *NIST SP 800-18*								

NOTES:

9. CONTINGENCY PLANNING

Contingency planning involves more than planning for a move offsite after a disaster destroys a facility. It also addresses how to keep an organization's critical functions operating in the event of disruptions, large and small. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Contingency Planning *OMB Circular A-130, III*								
9.1. Critical Element: Have the most critical and sensitive operations and their supporting computer resources been identified?								
9.1.1 Are critical data files and operations identified and the frequency of file backup documented? *FISCAM SC- SC-1.1 & 3.1 NIST SP 800-18*								
9.1.2 Are resources supporting critical operations identified? *FISCAM SC-1.2*								
9.1.3 Have processing priorities been established and approved by management? *FISCAM SC-1.3*								
9.2. Critical Element: Has a comprehensive contingency plan been developed and documented?								
9.2.1 Is the plan approved by key affected parties?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
FISCAM SC-3.1								
9.2.2 Are responsibilities for recovery assigned? *FISCAM SC-3.1*								
9.2.3 Are there detailed instructions for restoring operations? *FISCAM SC-3.1*								
9.2.4 Is there an alternate processing site; if so, is there a contract or interagency agreement in place? *FISCAM SC-3.1* *NIST SP 800-18*								
9.2.5 Is the location of stored backups identified? *NIST SP 800-18*								
9.2.6 Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged? *FISCAM SC-2.1*								
9.2.7 Is system and application documentation maintained at the off-site location? *FISCAM SC-2.1*								
9.2.8 Are all system defaults reset after being restored from a backup? *FISCAM SC-3.1*								
9.2.9 Are the backup storage site and alternate site geographically removed from the primary site and physically protected? *FISCAM SC-2.1*								
9.2.10 Has the contingency plan been distributed to all appropriate								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
personnel? *FISCAM SC-3.1*								
9.3. Critical Element: **Are tested contingency/disaster recovery plans in place?**								
9.3.1 Is an up-to-date copy of the plan stored securely off-site? *FISCAM SC-3.1*								
9.3.2 Are employees trained in their roles and responsibilities? *FISCAM SC-2.3* *NIST SP 800-18*								
9.3.3 Is the plan periodically tested and readjusted as appropriate? *FISCAM SC-3.1* *NIST SP 800-18*								

NOTES:

10. HARDWARE AND SYSTEM SOFTWARE MAINTENANCE

These are controls used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record is maintained of changes. Some of these controls are also covered in the Life Cycle Section. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Hardware and System Software Maintenance *OMB Circular A-130, III*								
10.1. Critical Element: Is access limited to system software and hardware?								
10.1.1 Are restrictions in place on who performs maintenance and repair activities? *OMB Circular A-130, III FISCAM SS-3.1 NIST SP 800-18*								
10.1.2 Is access to all program libraries restricted and controlled? *FISCAM CC-3.2 & 3.3*								
10.1.3 Are there on-site and off-site maintenance procedures (e.g., escort of maintenance personnel, sanitization of devices removed from the site)? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.1.4 Is the operating system configured to prevent circumvention of the security software and application controls? *FISCAM SS-1.2*								
10.1.5 Are up-to-date procedures in place for using and monitoring use of system utilities? *FISCAM SS-2.1*								
10.2. Critical Element: Are all new and revised hardware and software authorized, tested and approved before implementation?								
10.2.1 Is an impact analysis conducted to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control? *NIST SP 800-18*								
10.2.2 Are system components tested, documented, and approved (operating system, utility, applications) prior to promotion to production? *FISCAM SS-3.1, 3.2, & CC-2.1* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.2.3 Are software change request forms used to document requests and related approvals? *FISCAM CC-1.2 NIST SP 800-18*								
10.2..4 Are there detailed system specifications prepared and reviewed by management? *FISCAM CC-2.1*								
10.2.5 Is the type of test data to be used specified, i.e., live or made up? *NIST SP 800-18*								
10.2.6 Are default settings of security features set to the most restrictive mode? *PSN Security Assessment Guidelines*								
10.2.7 Are there software distribution implementation orders including effective date provided to all locations? *FISCAM CC-2.3*								
10.2.8 Is there version control? *NIST SP 800-18*								
10.2.9 Are programs labeled and inventoried? *FISCAM CC-3.1*								
10.2.10 Are the distribution and implementation of new or revised software documented and reviewed? *FISCAM SS-3.2*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.2.11 Are emergency change procedures documented and approved by management, either prior to the change or after the fact? *FISCAM CC-2.2*								
10.2.12 Are contingency plans and other associated documentation updated to reflect system changes? *FISCAM SC-2.1* *NIST SP 800-18*								
10.2.13 Is the use of copyrighted software or shareware and personally owned software/equipment documented? *NIST SP 800-18*								
10.3. Are systems managed to reduce vulnerabilities?								
10.3.1 Are systems periodically reviewed to identify and, when possible, eliminate unnecessary services (e.g., FTP, HTTP, mainframe supervisor calls)? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.3.2 Are systems periodically reviewed for known vulnerabilities and software patches promptly installed? *NIST SP 800-18*								

NOTES:

11. DATA INTEGRITY

Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user the information meets expectations about its quality and integrity. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Data Integrity *OMB Circular A-130, 8B3*								
11.1. Critical Element: Is virus detection and elimination software installed and activated?								
11.1.1 Are virus signature files routinely updated? *NIST SP 800-18*								
11.1.2 Are virus scans automatic? *NIST SP 800-18*								
11.2. Critical Element: Are data integrity and validation controls used to provide assurance that the information has not been altered and								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
the system functions as intended?								
11.2.1 Are reconciliation routines used by applications, i.e., checksums, hash totals, record counts? *NIST SP 800-18*								
11.2.2 Is inappropriate or unusual activity reported, investigated, and appropriate actions taken? *FISCAM SS-2.2*								
11.2.3 Are procedures in place to determine compliance with password policies? *NIST SP 800-18*								
11.2.4 Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions? *NIST SP 800-18*								
11.2.5 Are intrusion detection								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
tools installed on the system? *NIST SP 800-18*								
11.2.6 Are the intrusion detection reports routinely reviewed and suspected incidents handled accordingly? *NIST SP 800-18*								
11.2.7 Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks? *NIST SP 800-18*								
11.2.8 Is penetration testing performed on the system? *NIST SP 800-18*								
11.2.9 Is message authentication used? *NIST SP 800-18*								

NOTES:

12. DOCUMENTATION

The documentation contains descriptions of the hardware, software, policies, standards, procedures, and approvals related to the system and formalize the system's security controls. When answering whether there are procedures for each control objective, the question should be phrased "are there procedures for ensuring the documentation is obtained and maintained." The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Documentation *OMB Circular A-130, 8B3*								
12.1. Critical Element: Is there sufficient documentation that explains how software/hardware is to be used?								
12.1.1 Is there vendor-supplied documentation of purchased software? *NIST SP 800-18*								
12.1.2 Is there vendor-supplied documentation of purchased hardware? *NIST SP 800-18*								
12.1.3 Is there application documentation for in-house applications? *NIST SP 800-18*								
12.1.4 Are there network diagrams and documentation on setups of routers and switches? *NIST SP 800-18*								
12.1.5 Are there software and								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
hardware testing procedures and results? *NIST SP 800-18*								
12.1.6 Are there standard operating procedures for all the topic areas covered in this document? *NIST SP 800-18*								
12.1.7 Are there user manuals? *NIST SP 800-18*								
12.1.8 Are there emergency procedures? *NIST SP 800-18*								
12.1.9 Are there backup procedures? *NIST SP 800-18*								
12.2. Critical Element: Are there formal security and operational procedures documented?								
12.2.1 Is there a system security plan? *OMB Circular A-130, III* *FISCAM SP-2.1* *NIST SP 800-18*								
12.2.2 Is there a contingency plan? *NIST SP 800-18*								
12.2.3 Are there written agreements regarding how data is shared between interconnected systems? *OMB A-130, III* *NIST SP 800-18*								
12.2.4 Are there risk assessment reports? *NIST SP 800-18*								
12.2.5 Are there certification and accreditation documents and a								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
statement authorizing the system to process? *NIST SP 800-18*								

NOTES:

13. SECURITY AWARENESS, TRAINING, AND EDUCATION

People are a crucial factor in ensuring the security of computer systems and valuable information resources. Security awareness, training, and education enhance security by improving awareness of the need to protect system resources. Additionally, training develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Security Awareness, Training, and Education *OMB Circular A-130, III*								
13.1. Critical Element: Have employees received adequate training to fulfill their security responsibilities?								
13.1.1 Have employees received a copy of the Rules of Behavior? *NIST SP 800-18*								
13.1.2 Are employee training and professional development documented and monitored? *FISCAM SP-4.2*								
13.1.3 Is there mandatory annual refresher training? *OMB Circular A-130, III*								
13.1.4 Are methods employed to								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
make employees aware of security, i.e., posters, booklets? *NIST SP 800-18*								
13.1.5 Have employees received a copy of or have easy access to agency security procedures and policies? *NIST SP 800-18*								

NOTES:

14. INCIDENT RESPONSE CAPABILITY

Computer security incidents are an adverse event in a computer system or network. Such incidents are becoming more common and their impact far-reaching. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Incident Response Capability *OMB Circular A-130, III FISCAM SP-3.4 NIST 800-18*								
14.1. Critical Element: Is there a capability to provide help to users when a security incident occurs in the system?								
14.1.1 Is a formal incident response capability available? *FISCAM SP-3.4 NIST SP 800-18*								
14.1.2 Is there a process for reporting incidents? *FISCAM SP-3.4 NIST SP 800-18*								
14.1.3 Are incidents monitored and tracked until resolved? *NIST SP 800-18*								
14.1.4 Are personnel trained to recognize and handle incidents? *FISCAM SP-3.4 NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
14.1.5 Are alerts/advisories received and responded to? *NIST SP 800-18*								
14.1.6 Is there a process to modify incident handling procedures and control techniques after an incident occurs? *NIST SP 800-18*								
14.2. Critical Element: Is incident related information shared with appropriate organizations?								
14.2.1 Is incident information and common vulnerabilities or threats shared with owners of interconnected systems? *OMB A-130, III NIST SP 800-18*								
14.2.2 Is incident information shared with FedCIRC[2] concerning incidents and common vulnerabilities and threats? *OMB A-130, III GISRA*								
14.2.3 Is incident information reported to								

2 FedCIRC (Federal Computer Incident Response Capability) is the U.S. Government's focal point for handling computer security-related incidents.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
FedCIRC, NIPC[3], and local law enforcement when necessary? *OMB A-130,III GISRA*								

NOTES:

TECHNICAL CONTROLS

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

15. IDENTIFICATION AND AUTHENTICATION

Identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Identification and Authentication *OMB Circular A-130, III FISCAM AC-2 NIST SP 800-18*								
15.1. Critical Element: Are users individually authenticated								

[3] NIPC's mission is to serve as the U.S. Government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
via passwords, tokens, or other devices?								
15.1.1 Is a current list maintained and approved of authorized users and their access? *FISCAM AC-2 NIST SP 800-18*								
15.1.2 Are digital signatures used and conform to FIPS 186-2? *NIST SP 800-18*								
15.1.3 Are access scripts with embedded passwords prohibited? *NIST SP 800-18*								
15.1.4 Is emergency and temporary access authorized? *FISCAM AC-2.2*								
15.1.5 Are personnel files matched with user accounts to ensure that terminated or transferred individuals do not retain system access? *FISCAM AC-3.2*								
15.1.6 Are passwords changed at least every ninety days or earlier if needed? *FISCAM AC-3.2 NIST SP 800-18*								
15.1.7 Are passwords unique and difficult to guess (e.g., do passwords require alpha numeric, upper/lower case, and special								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
characters)? *FISCAM AC-3.2 NIST SP 800-18*								
15.1.8 Are inactive user identifications disabled after a specified period of time? *FISCAM AC-3.2 NIST SP 800-18*								
15.1.9 Are passwords not displayed when entered? *FISCAM AC-3.2 NIST SP 800-18*								
15.1.10 Are there procedures in place for handling lost and compromised passwords? *FISCAM AC-3.2 NIST SP 800-18*								
15.1.11 Are passwords distributed securely and users informed not to reveal their passwords to anyone (social engineering)? *NIST SP 800-18*								
15.1.12 Are passwords transmitted and stored using secure protocols/algorithms? *FISCAM AC-3.2 NIST SP 800-18*								
15.1.13 Are vendor-supplied passwords replaced immediately? *FISCAM AC-3.2 NIST SP 800-18*								
15.1.14 Is there a limit to the number of invalid access attempts that may occur								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
for a given user? *FISCAM AC-3.2 NIST SP 800-18*								
15.2. Critical Element: Are access controls enforcing segregation of duties?								
15.2.1 Does the system correlate actions to users? *OMB A-130, III FISCAM SD-2.1*								
15.2.2 Do data owners periodically review access authorizations to determine whether they remain appropriate? *FISCAM AC-2.1*								

NOTES:

16. LOGICAL ACCESS CONTROLS

Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Logical Access Controls *OMB Circular A-130, III* *FISCAM AC-3.2* *NIST SP 800-18*								
16.1. Critical Element: Do the logical access controls restrict users to authorized transactions and functions?								
16.1.1 Can the security controls detect unauthorized access attempts? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.2 Is there access control software that prevents an individual from having all necessary authority or information access to allow fraudulent activity without collusion? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.3 Is access to security software restricted to security administrators? *FISCAM AC-3.2*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.1.4 Do workstations disconnect or screen savers lock system after a specific period of inactivity? *FISCAM AC-3.2* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.1.5 Are inactive users' accounts monitored and removed when not needed? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.6 Are internal security labels (naming conventions) used to control access to specific information types or files? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.7 If encryption is used, does it meet federal standards? *NIST SP 800-18*								
16.1.8 If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving? *NIST SP 800-18*								
16.1.9 Is access restricted to files at the logical view or field? *FISCAM AC-3.2*								
16.1.10 Is access monitored to identify apparent security violations and are such events investigated? *FISCAM AC-4*								
16.2. Critical Element: **Are there logical controls over network access?**								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.2.1 Has communication software been implemented to restrict access through specific terminals? *FISCAM AC-3.2*								
16.2.2 Are insecure protocols (e.g., UDP, ftp) disabled? *PSN Security Assessment Guidelines*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.2.3 Have all vendor-supplied default security parameters been reinitialized to more secure settings? *PSN Security Assessment Guidelines*								
16.2.4 Are there controls that restrict remote access to the system? *NIST SP 800-18*								
16.2.5 Are network activity logs maintained and reviewed? *FISCAM AC-3.2*								
16.2.6 Does the network connection automatically disconnect at the end of a session? *FISCAM AC-3.2*								
16.2.7 Are trust relationships among hosts and external entities appropriately restricted? *PSN Security Assessment Guidelines*								
16.2.8 Is dial-in access monitored? *FISCAM AC-3.2*								
16.2.9 Is access to telecommunications hardware or facilities restricted and monitored? *FISCAM AC-3.2*								
16.2.10 Are firewalls or secure gateways installed? *NIST SP 800-18*								
16.2.11 If firewalls are installed do they comply with firewall policy and rules?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
FISCAM AC-3.2								
16.2.12 Are guest and anonymous accounts authorized and monitored? *PSN Security Assessment Guidelines*								
16.2.13 Is an approved standardized log-on banner displayed on the system warning unauthorized users that they have accessed a U.S. Government system and can be punished? *FISCAM AC-3.2 NIST SP 800-18*								
16.2.14 Are sensitive data transmissions encrypted? *FISCAM AC-3.2*								
16.2.15 Is access to tables defining network options, resources, and operator profiles restricted? *FISCAM AC-3.2*								
16.3. Critical Element: If the public accesses the system, are there controls implemented to protect the integrity of the application and the confidence of the public?								
16.3.1 Is a privacy policy posted on the web site? *OMB-99-18*								

NOTES:

17. AUDIT TRAILS

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems. The following questions are organized under one critical element. The levels for the critical element should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Audit Trails *OMB Circular A-130, III FISCAM AC-4.1 NIST SP 800-18*								
17.1. Critical Element: Is activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated?								
17.1.1 Does the audit trail provide a trace of user actions? *NIST SP 800-18*								
17.1.2 Can the audit trail support after-the-fact investigations of how, when, and why normal operations ceased? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
17.1.3 Is access to online audit logs strictly controlled? *NIST SP 800-18*								
17.1.4 Are off-line storage of audit logs retained for a period of time, and if so, is access to audit logs strictly controlled? *NIST SP 800-18*								
17.1.5 Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail? *NIST SP 800-18*								
17.1.6 Are audit trails reviewed frequently? *NIST SP 800-18*								
17.1.7 Are automated tools used to review audit records in real time or near real time? *NIST SP 800-18*								
17.1.8 Is suspicious activity investigated								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
and appropriate action taken? *FISCAM AC-4.3*								
17.1.9 Is keystroke monitoring used? If so, are users notified? *NIST SP 800-18*								

NOTES:

APPENDIX B. PRELIMINARY VULNERABILIY ASSESSMENT CHECKLIST FOR DON SCADA SYSTEMS

System Name, Title, and Unique Identifier: _____

Major Application _____ or General Support System _____

NAME OF ASSESSORS:

_____

_____

_____

Date of Evaluation: _____

List of Connected Systems:

Name of System	Are boundary controls effective?	Planned action if not effective
1.		
2.		
3.		

Criticality of System	Category of Sensitivity High, Medium, or Low
Confidentiality	
Integrity	
Availability	

Purpose and Objective of Assessment: _____

_____

_____

MANAGEMENT CONTROLS

Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management.

1. RISK MANAGEMENT

Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Risk Management *OMB Circular A-130, III*								
1.1 Critical Element: Is risk periodically assessed?								
1.1.1 Is the current system configuration documented, including links to other systems? *NIST SP 800-18*								
1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change? *FISCAM SP-1*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
1.1.3 Has data sensitivity and integrity of the data been considered? *FISCAM SP-1*								
1.1.4 Have threat sources, both natural and manmade, been identified? *FISCAM SP-1*								
1.1.5 Has a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources been developed and maintained current? *NIST SP 800-30*[4]								
1.1.6 Has an analysis been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities? *NIST SP 800-30*								
1.2. Critical Element: Do program officials understand the risk to systems under their control and determine the acceptable level of risk?								

4 Draft NIST Special Publication 800-30, "Risk Management Guidance" dated June 2001.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
1.2.1 Are final risk determinations and related management approvals documented and maintained on file? *FISCAM SP-1*								
1.2.2 Has a mission/business impact analysis been conducted? *NIST SP 800-30*								
1.2.3 Have additional controls been identified to sufficiently mitigate identified risks? *NIST SP 800-30*								

NOTES:

2. REVIEW OF SECURITY CONTROLS

Routine evaluations and response to identified vulnerabilities are important elements of managing the risk of a system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Review of Security Controls *OMB Circular A-130, III FISCAM SP-5 NIST SP 800-18*								
2.1. Critical Element: **Have the security controls of the system and interconnected systems been reviewed?**								
2.1 1 Has the system and all network boundaries been subjected to periodic reviews? *FISCAM SP-5.1*								
2.1.2 Has an independent review been performed when a significant change occurred? *OMB Circular A-130, III FISCAM SP-5.1 NIST SP 800-*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
18								
2.1.3 Are routine self-assessments conducted ? *NIST SP 800-18*								
2.1.4 Are tests and examinations of key controls routinely made, i.e., network scans, analyses of router and switch settings, penetration testing? *OMB Circular A-130, 8B3* *NIST SP 800-18*								
2.1.5 Are security alerts and security incidents analyzed and remedial actions taken? *FISCAM SP 3-4* *NIST SP 800-18*								
2.2. Critical Element: Does management ensure that corrective actions are effectively implemented?								
2.2.1 Is there an effective and timely process for reporting significant weakness and ensuring effective								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
remedial action? *FISCAM SP 5-1 and 5.2 NIST SP 800-18*								

NOTES:

3. LIFE CYCLE

Like other aspects of an IT system, security is best managed if planned for throughout the IT system life cycle. There are many models for the IT system life cycle but most contain five basic phases: initiation, development/acquisition, implementation, operation, and disposal. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Life Cycle *OMB Circular A-130, III* *FISCAM CC-1.1*								
3.1. Critical Element: **Has a system development life cycle methodology been developed?**								
Initiation Phase								
Development/Acquisition Phase								
Implementation Phase								
3.2. Critical Element: Are changes controlled as programs progress through testing to final approval?								
3.2.1 Are design reviews and system tests run prior to placing the system in production? *FISCAM CC-2.1* *NIST SP 800-18*								
3.2.2 Are the test results documented? *FISCAM CC-2.1* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.2.3 Is certification testing of security controls conducted and documented? *NIST SP 800-18*								
3.2.4 If security controls were added since development, has the system documentation been modified to include them? *NIST SP 800-18*								
3.2.5 If security controls were added since development, have the security controls been tested and the system recertified? *FISCAM CC-2.1* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.2.6 Has the application undergone a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards? *NIST SP 800-18*								
3.2.7 Does the system have written authorization to operate either on an interim basis with planned corrective action or full authorization? *NIST SP 800-18*								
Operation/Maintenance Phase								
3.2.8 Has a system security plan been developed and approved? *OMB Circular A-130, III* *FISCAM SP 2-1* *NIST SP 800-18*								
3.2.9 If the system connects to other systems, have controls been established and disseminated to the owners of the interconnected systems? *NIST SP 800-18*								
3.2.10 Is the system security plan kept current? *OMB Circular A-130, III* *FISCAM SP 2-1* *NIST SP 800-18*								
Disposal Phase								
3.2.11 Are official electronic records properly disposed/archived? NIST SP 800-18								
3.2.12 Is information or media purged, overwritten, degaussed, or destroyed when disposed or used elsewhere? *FISCAM AC-3.4* *NIST SP 800-18*								
3.2.13 Is a record kept of who implemented the								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
disposal actions and verified that the information or media was sanitized? *NIST SP 800-18*								

NOTES:

4. AUTHORIZE PROCESSING (CERTIFICATION & ACCREDITATION)

Authorize processing (Note: Some agencies refer to this process as certification and accreditation) provides a form of assurance of the security of the system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Authorize Processing (Certification & Accreditation) *OMB Circular A-130, III FIPS 102*								
4.1. Critical Element: Has the system been certified/recertified and authorized to process (accredited)?								
4.1.1 Has a technical and/or security evaluation been completed or conducted when a significant change occurred? *NIST SP 800-18*								
4.1.2 Has a risk assessment been conducted when a significant change occurred? *NIST SP 800-18*								
4.1.3 Have Rules of Behavior been established and signed by users? *NIST SP 800-18*								
4.1.4 Has a contingency plan been developed and tested? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
4.1.5 Has a system security plan been developed, updated, and reviewed? *NIST SP 800-18*								
4.1.6 Are in-place controls operating as intended? *NIST SP 800-18*								
4.1.7 Are the planned and in-place controls consistent with the identified risks and the system and data sensitivity? *NIST SP 800-18*								
4.1.8 Has management authorized interconnections to all systems (including systems owned and operated by another program, agency, organization or contractor)? *NIST 800-18*								
4.2. Critical Element: Is the system operating on an interim authority to process in accordance with specified agency procedures?								
4.2.1 Has management initiated prompt action to correct deficiencies? *NIST SP 800-18*								

NOTES:

5. SYSTEM SECURITY PLAN

System security plans provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The plan delineates responsibilities and expected behavior of all individuals who access the system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
System security plan *OMB Circular A-130, III NIST SP 800-18 FISCAM SP-2.1*								
5.1. Critical Element: Is a system security plan documented for the system and all interconnected systems if the boundary controls are ineffective?								
5.1.1 Is the system security plan approved by key affected parties and management? *FISCAM SP-2.1 NIST SP 800-18*								
5.1.2 Does the plan contain the topics prescribed in NIST Special Publication 800-18? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
5.1.3 Is a summary of the plan incorporated into the strategic IRM plan? *OMB Circular A-130, III* *NIST SP 800-18*								
5.2. Critical Element: Is the plan kept current?								
5.2.1 Is the plan reviewed periodically and adjusted to reflect current conditions and risks? *FISCAM SP-2.1* *NIST SP 800-18*								

NOTES:

OPERATIONAL CONTROLS

The operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls.

6. PERSONNEL SECURITY

Many important issues in computer security involve human users, designers, implementers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives	**L.1** Policy	**L.2** Procedures	**L.3** Implemented	**L.4** Tested	**L.5** Integrated	**Risk Based Decision Made**	**Comments**	**Initials**
Personnel Security *OMB Circular A-130, III*								
6.1. Critical Element: Are duties separated to ensure least privilege and individual accountability?								
6.1.1 Are all positions reviewed for sensitivity level? *FISCAM SD-1.2 NIST SP 800-18*								
6.1.2 Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties? *FISCAM SD-1.2*								

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
6.1.3 Are sensitive functions divided among different individuals? *OMB Circular A-130, III FISCAM SD-1 NIST SP 800-18*								
6.1.4 Are distinct systems support functions performed by different individuals? *FISCAM SD-1.1*								
6.1.5 Are mechanisms in place for holding users responsible for their actions? *OMB Circular A-130, III FISCAM SD-2 & 3.2*								
6.1.6 Are regularly scheduled vacations and periodic job/shift rotations required? *FISCAM SD-1.1 FISCAM SP-4.1*								
6.1.7 Are hiring, transfer, and termination procedures established? *FISCAM SP-4.1 NIST SP 800-18*								
6.1.8 Is there a process for requesting, establishing, issuing, and closing user accounts? *FISCAM SP-4.1*								

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
NIST 800-18								
6.2. Critical Element: **Is appropriate background screening for assigned positions completed prior to granting access?**								
6.2.1 Are individuals who are authorized to bypass significant technical and operational controls screened prior to access and periodically thereafter? *OMB Circular A-130, III FISCAM SP-4.1*								
6.2.2 Are confidentiality or security agreements required for employees assigned to work with sensitive information? *FISCAM SP-4.1*								
6.2.3 When controls cannot adequately protect the information, are individuals screened prior to access? *OMB Circular A-130, III*								
6.2.4 Are there conditions for allowing system access prior to								

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
completion of screening? *FISCAM AC-2.2 NIST SP 800-18*								

NOTES:

7. PHYSICAL AND ENVIRONMENTAL PROTECTION

Physical security and environmental security are the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Physical and Environmental Protection								
Physical Access Control								
7.1. Critical Element: Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?								
7.1.1 Is access to facilities controlled through the use of guards, identification badges, or entry devices such as key cards or biometrics? *FISCAM AC-3 NIST SP 800-18*								
7.1.2 Does management regularly review the list of persons with physical access								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
to sensitive facilities? *FISCAM AC-3.1*								
7.1.3 Are deposits and withdrawals of tapes and other storage media from the library authorized and logged? *FISCAM AC-3.1*								
7.1.4 Are keys or other access devices needed to enter the computer room and tape/media library? *FISCAM AC-3.1*								
7.1.5 Are unused keys or other entry devices secured? *FISCAM AC-3.1*								
7.1.6 Do emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter after fire drills, etc? *FISCAM AC-3.1*								
7.1.7 Are visitors to sensitive areas signed in and escorted? *FISCAM AC-3.1*								
7.1.8 Are entry codes changed periodically? *FISCAM AC-3.1*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
7.1.9 Are physical accesses monitored through audit trails and apparent security violations investigated and remedial action taken? *FISCAM AC-4*								
7.1.10 Is suspicious access activity investigated and appropriate action taken? *FISCAM AC-4.3*								
7.1.11 Are visitors, contractors and maintenance personnel authenticated through the use of preplanned appointments and identification checks? *FISCAM AC-3.1*								
Fire Safety Factors								
7.1.12 Are appropriate fire suppression and prevention devices installed and working? *FISCAM SC-2.2* *NIST SP 800-18*								
7.1.13 Are fire ignition sources, such as failures of electronic devices								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
or wiring, improper storage materials, and the possibility of arson, reviewed periodically? *NIST SP 800-18*								
Supporting Utilities								
7.1.14 Are heating and air-conditioning systems regularly maintained? *NIST SP 800-18*								
7.1.15 Is there a redundant air-cooling system? *FISCAM SC-2.2*								
7.1.16 Are electric power distribution, heating plants, water, sewage, and other utilities periodically reviewed for risk of failure? *FISCAM SC-2.2* *NIST SP 800-18*								
7.1.17 Are building plumbing lines known and do not endanger system? *FISCAM SC-2.2* *NIST SP 800-18*								
7.1.18 Has an uninterruptible power supply or backup								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
generator been provided? *FISCAM SC-2.2*								
7.1.19 Have controls been implemented to mitigate other disasters, such as floods, earthquakes, etc.? *FISCAM SC-2.2*								
Interception of Data								
7.2. Critical Element: Is data protected from interception?								
7.2.1 Are computer monitors located to eliminate viewing by unauthorized persons? *NIST SP 800-18*								
7.2.2 Is physical access to data transmission lines controlled? *NIST SP 800-18*								
Mobile and Portable Systems								
7.3. Critical Element: Are mobile and portable systems protected?								
7.3.1 Are sensitive data files encrypted on all portable systems?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
NIST SP 800-14								
7.3.2 Are portable systems stored securely? *NIST SP 800-14*								

NOTES:

8. PRODUCTION, INPUT/OUTPUT CONTROLS

There are many aspects to supporting IT operations. Topics range from a user help desk to procedures for storing, handling and destroying media. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Production, Input/Output Controls								
8.1. Critical Element: Is there user support?								
8.1.1 Is there a help desk or group that offers advice? *NIST SP 800-18*								
8.2. Critical Element: Are there media controls?								
8.2.1 Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information? *NIST SP 800-18*								
8.2.2 Are there processes for ensuring that only authorized users pick up, receive, or deliver input and output information and media?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
NIST SP 800-18								
8.2.3 Are audit trails used for receipt of sensitive inputs/outputs? *NIST SP 800-18*								
8.2.4 Are controls in place for transporting or mailing media or printed output? *NIST SP 800-18*								
8.2.5 Is there internal/external labeling for sensitivity? *NIST SP 800-18*								
8.2.6 Is there external labeling with special handling instructions? *NIST SP 800-18*								
8.2.7 Are audit trails kept for inventory management? *NIST SP 800-18*								
8.2.8 Is media sanitized for reuse? *FISCAM AC-3.4* *NIST SP 800-18*								
8.2.9 Is damaged media stored and /or								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
destroyed? *NIST SP 800-18*								
8.2.10 Is hardcopy media shredded or destroyed when no longer needed? *NIST SP 800-18*								

NOTES:

9. CONTINGENCY PLANNING

Contingency planning involves more than planning for a move offsite after a disaster destroys a facility. It also addresses how to keep an organization's critical functions operating in the event of disruptions, large and small. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Contingency Planning *OMB Circular A-130, III*								
9.1. Critical Element: Have the most critical and sensitive operations and their supporting computer resources been identified?								
9.1.1 Are critical data files and operations identified and the frequency of file backup documented? *FISCAM SC- SC-1.1 & 3.1 NIST SP 800-18*								
9.1.2 Are resources supporting critical operations identified? *FISCAM SC-1.2*								
9.1.3 Have processing priorities been established and approved by management? *FISCAM SC-1.3*								
9.2. Critical Element: Has a comprehensive contingency plan been developed and documented?								
9.2.1 Is the plan approved by key affected parties?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
FISCAM SC-3.1								
9.2.2 Are responsibilities for recovery assigned? *FISCAM SC-3.1*								
9.2.3 Are there detailed instructions for restoring operations? *FISCAM SC-3.1*								
9.2.4 Is there an alternate processing site; if so, is there a contract or interagency agreement in place? *FISCAM SC-3.1* *NIST SP 800-18*								
9.2.5 Is the location of stored backups identified? *NIST SP 800-18*								
9.2.6 Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged? *FISCAM SC-2.1*								
9.2.7 Is system and application documentation maintained at the off-site location? *FISCAM SC-2.1*								
9.2.8 Are all system defaults reset after being restored from a backup? *FISCAM SC-3.1*								
9.2.9 Are the backup storage site and alternate site geographically removed from the primary site and physically protected? *FISCAM SC-2.1*								
9.2.10 Has the contingency plan been distributed to all appropriate								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
personnel? *FISCAM SC-3.1*								
9.3. Critical Element: Are tested contingency/disaster recovery plans in place?								
9.3.1 Is an up-to-date copy of the plan stored securely off-site? *FISCAM SC-3.1*								
9.3.2 Are employees trained in their roles and responsibilities? *FISCAM SC-2.3* *NIST SP 800-18*								
9.3.3 Is the plan periodically tested and readjusted as appropriate? *FISCAM SC-3.1* *NIST SP 800-18*								

NOTES:

10. HARDWARE AND SYSTEM SOFTWARE MAINTENANCE

These are controls used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record is maintained of changes. Some of these controls are also covered in the Life Cycle Section. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Hardware and System Software Maintenance *OMB Circular A-130, III*								
10.1. Critical Element: Is access limited to system software and hardware?								
10.1.1 Are restrictions in place on who performs maintenance and repair activities? *OMB Circular A-130, III FISCAM SS-3.1 NIST SP 800-18*								
10.1.2 Is access to all program libraries restricted and controlled? *FISCAM CC-3.2 & 3.3*								
10.1.3 Are there on-site and off-site maintenance procedures (e.g., escort of maintenance personnel, sanitization of devices removed from the site)? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.1.4 Is the operating system configured to prevent circumvention of the security software and application controls? *FISCAM SS-1.2*								
10.1.5 Are up-to-date procedures in place for using and monitoring use of system utilities? *FISCAM SS-2.1*								
10.2. Critical Element: Are all new and revised hardware and software authorized, tested and approved before implementation?								
10.2.1 Is an impact analysis conducted to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control? *NIST SP 800-18*								
10.2.2 Are system components tested, documented, and approved (operating system, utility, applications) prior to promotion to production? *FISCAM SS-3.1, 3.2, & CC-2.1* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.2.3 Are software change request forms used to document requests and related approvals? *FISCAM CC-1.2 NIST SP 800-18*								
10.2..4 Are there detailed system specifications prepared and reviewed by management? *FISCAM CC-2.1*								
10.2.5 Is the type of test data to be used specified, i.e., live or made up? *NIST SP 800-18*								
10.2.6 Are default settings of security features set to the most restrictive mode? *PSN Security Assessment Guidelines*								
10.2.7 Are there software distribution implementation orders including effective date provided to all locations? *FISCAM CC-2.3*								
10.2.8 Is there version control? *NIST SP 800-18*								
10.2.9 Are programs labeled and inventoried? *FISCAM CC-3.1*								
10.2.10 Are the distribution and implementation of new or revised software documented and reviewed? *FISCAM SS-3.2*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.2.11 Are emergency change procedures documented and approved by management, either prior to the change or after the fact? *FISCAM CC-2.2*								
10.2.12 Are contingency plans and other associated documentation updated to reflect system changes? *FISCAM SC-2.1* *NIST SP 800-18*								
10.2.13 Is the use of copyrighted software or shareware and personally owned software/equipment documented? *NIST SP 800-18*								
10.3. Are systems managed to reduce vulnerabilities?								
10.3.1 Are systems periodically reviewed to identify and, when possible, eliminate unnecessary services (e.g., FTP, HTTP, mainframe supervisor calls)? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.3.2 Are systems periodically reviewed for known vulnerabilities and software patches promptly installed? *NIST SP 800-18*								

NOTES:

11. DATA INTEGRITY

Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user the information meets expectations about its quality and integrity. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Data Integrity *OMB Circular A-130, 8B3*								
11.1. Critical Element: Is virus detection and elimination software installed and activated?								
11.1.1 Are virus signature files routinely updated? *NIST SP 800-18*								
11.1.2 Are virus scans automatic? *NIST SP 800-18*								
11.2. Critical Element: Are data integrity and validation controls used to provide assurance that the information has not been altered and								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
the system functions as intended?								

NOTES:

12. DOCUMENTATION

The documentation contains descriptions of the hardware, software, policies, standards, procedures, and approvals related to the system and formalize the system's security controls. When answering whether there are procedures for each control objective, the question should be phrased "are there procedures for ensuring the documentation is obtained and maintained." The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Documentation *OMB Circular A-130, 8B3*								
12.1. Critical Element: Is there sufficient documentation that explains how software/hardware is to be used?								
12.1.1 Is there vendor-supplied documentation of purchased software? *NIST SP 800-18*								
12.1.2 Is there vendor-supplied documentation of purchased hardware? *NIST SP 800-18*								
12.1.3 Is there application documentation for in-house applications? *NIST SP 800-18*								
12.1.4 Are there network diagrams and documentation on setups of routers and switches? *NIST SP 800-18*								
12.1.5 Are there software and hardware testing procedures and results?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
NIST SP 800-18								
12.1.6 Are there standard operating procedures for all the topic areas covered in this document? *NIST SP 800-18*								
12.1.7 Are there user manuals? *NIST SP 800-18*								
12.1.8 Are there emergency procedures? *NIST SP 800-18*								
12.1.9 Are there backup procedures? *NIST SP 800-18*								
12.2. Critical Element: Are there formal security and operational procedures documented?								
12.2.1 Is there a system security plan? *OMB Circular A-130, III* *FISCAM SP-2.1* *NIST SP 800-18*								
12.2.2 Is there a contingency plan? *NIST SP 800-18*								
12.2.3 Are there written agreements regarding how data is shared between interconnected systems? *OMB A-130, III* *NIST SP 800-18*								
12.2.4 Are there risk assessment reports? *NIST SP 800-18*								
12.2.5 Are there certification and accreditation documents and a statement authorizing the								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
system to process? *NIST SP 800-18*								

NOTES:

13. SECURITY AWARENESS, TRAINING, AND EDUCATION

People are a crucial factor in ensuring the security of computer systems and valuable information resources. Security awareness, training, and education enhance security by improving awareness of the need to protect system resources. Additionally, training develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Security Awareness, Training, and Education *OMB Circular A-130, III*								
13.1. Critical Element: Have employees received adequate training to fulfill their security responsibilities?								
13.1.1 Have employees received a copy of the Rules of Behavior? *NIST SP 800-18*								
13.1.2 Are employee training and professional development documented and monitored? *FISCAM SP-4.2*								
13.1.3 Is there mandatory annual refresher training? *OMB Circular A-130, III*								
13.1.4 Are methods employed to								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
make employees aware of security, i.e., posters, booklets? *NIST SP 800-18*								
13.1.5 Have employees received a copy of or have easy access to agency security procedures and policies? *NIST SP 800-18*								

NOTES:

14. INCIDENT RESPONSE CAPABILITY

Computer security incidents are an adverse event in a computer system or network. Such incidents are becoming more common and their impact far-reaching. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Incident Response Capability *OMB Circular A-130, III FISCAM SP-3.4 NIST 800-18*								
14.1. Critical Element: Is there a capability to provide help to users when a security incident occurs in the system?								
14.1.1 Is a formal incident response capability available? *FISCAM SP-3.4 NIST SP 800-18*								
14.1.2 Is there a process for reporting incidents? *FISCAM SP-3.4 NIST SP 800-18*								
14.1.3 Are incidents monitored and tracked until resolved? *NIST SP 800-18*								
14.1.4 Are personnel trained to recognize and handle incidents? *FISCAM SP-3.4 NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
14.1.5 Are alerts/advisories received and responded to? *NIST SP 800-18*								
14.1.6 Is there a process to modify incident handling procedures and control techniques after an incident occurs? *NIST SP 800-18*								
14.2. Critical Element: Is incident related information shared with appropriate organizations?								
14.2.1 Is incident information and common vulnerabilities or threats shared with owners of interconnected systems? *OMB A-130, III NIST SP 800-18*								
14.2.2 Is incident information shared with FedCIRC[5] concerning incidents and common vulnerabilities and threats? *OMB A-130, III GISRA*								
14.2.3 Is incident information reported to								

5 FedCIRC (Federal Computer Incident Response Capability) is the U.S. Government's focal point for handling computer security-related incidents.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
FedCIRC, NIPC[6], and local law enforcement when necessary? *OMB A-130,III GISRA*								

NOTES:

6 NIPC's mission is to serve as the U.S. Government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures.

TECHNICAL CONTROLS

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

15. IDENTIFICATION AND AUTHENTICATION

Identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Identification and Authentication *OMB Circular A-130, III FISCAM AC-2 NIST SP 800-18*								
15.1. Critical Element: Are users individually authenticated via passwords, tokens, or other devices?								
15.1.1 Is a current list maintained and approved of authorized users and their access? *FISCAM AC-2 NIST SP 800-18*								
15.1.2 Are digital signatures used and conform to FIPS 186-2? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
15.1.3 Are access scripts with embedded passwords prohibited? *NIST SP 800-18*								
15.1.4 Is emergency and temporary access authorized? *FISCAM AC-2.2*								
15.1.5 Are personnel files matched with user accounts to ensure that terminated or transferred individuals do not retain system access? *FISCAM AC-3.2*								
15.1.6 Are passwords changed at least every ninety days or earlier if needed? *FISCAM AC-3.2 NIST SP 800-18*								
15.1.7 Are passwords unique and difficult to guess (e.g., do passwords require alpha numeric, upper/lower case, and special characters)? *FISCAM AC-3.2 NIST SP 800-18*								
15.1.8 Are inactive user identifications disabled after a specified period of time? *FISCAM AC-3.2 NIST SP 800-18*								
15.1.9 Are passwords not displayed when entered? *FISCAM AC-3.2*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
NIST SP 800-18								
15.1.10 Are there procedures in place for handling lost and compromised passwords? *FISCAM AC-3.2 NIST SP 800-18*								
15.1.11 Are passwords distributed securely and users informed not to reveal their passwords to anyone (social engineering)? *NIST SP 800-18*								
15.1.12 Are passwords transmitted and stored using secure protocols/algorithms? *FISCAM AC-3.2 NIST SP 800-18*								
15.1.13 Are vendor-supplied passwords replaced immediately? *FISCAM AC-3.2 NIST SP 800-18*								
15.1.14 Is there a limit to the number of invalid access attempts that may occur for a given user? *FISCAM AC-3.2 NIST SP 800-18*								
15.2. Critical Element: Are access controls enforcing segregation of duties?								
15.2.1 Does the system correlate actions to users? *OMB A-130, III FISCAM SD-2.1*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
15.2.2 Do data owners periodically review access authorizations to determine whether they remain appropriate? *FISCAM AC-2.1*								

NOTES:

16. LOGICAL ACCESS CONTROLS

Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Logical Access Controls *OMB Circular A-130, III* *FISCAM AC-3.2* *NIST SP 800-18*								
16.1. Critical Element: Do the logical access controls restrict users to authorized transactions and functions?								
16.1.1 Can the security controls detect unauthorized access attempts? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.2 Is there access control software that prevents an individual from having all necessary authority or information access to allow fraudulent activity without collusion? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.3 Is access to security software restricted to security administrators? *FISCAM AC-3.2*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.1.4 Do workstations disconnect or screen savers lock system after a specific period of inactivity? *FISCAM AC-3.2* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.1.5 Are inactive users' accounts monitored and removed when not needed? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.6 Are internal security labels (naming conventions) used to control access to specific information types or files? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.7 If encryption is used, does it meet federal standards? *NIST SP 800-18*								
16.1.8 If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving? *NIST SP 800-18*								
16.1.9 Is access restricted to files at the logical view or field? *FISCAM AC-3.2*								
16.1.10 Is access monitored to identify apparent security violations and are such events investigated? *FISCAM AC-4*								
16.2. Critical Element: **Are there logical controls over network access?**								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.2.1 Has communication software been implemented to restrict access through specific terminals? *FISCAM AC-3.2*								
16.2.2 Are insecure protocols (e.g., UDP, ftp) disabled? *PSN Security Assessment Guidelines*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.2.3 Have all vendor-supplied default security parameters been reinitialized to more secure settings? *PSN Security Assessment Guidelines*								
16.2.4 Are there controls that restrict remote access to the system? *NIST SP 800-18*								
16.2.5 Are network activity logs maintained and reviewed? *FISCAM AC-3.2*								
16.2.6 Does the network connection automatically disconnect at the end of a session? *FISCAM AC-3.2*								
16.2.7 Are trust relationships among hosts and external entities appropriately restricted? *PSN Security Assessment Guidelines*								
16.2.8 Is dial-in access monitored? *FISCAM AC-3.2*								
16.2.9 Is access to telecommunications hardware or facilities restricted and monitored? *FISCAM AC-3.2*								
16.2.10 Are firewalls or secure gateways installed? *NIST SP 800-18*								
16.2.11 If firewalls are installed do they comply with firewall policy and rules?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
FISCAM AC-3.2								
16.2.12 Are guest and anonymous accounts authorized and monitored? *PSN Security Assessment Guidelines*								
16.2.13 Is an approved standardized log-on banner displayed on the system warning unauthorized users that they have accessed a U.S. Government system and can be punished? *FISCAM AC-3.2 NIST SP 800-18*								
16.2.14 Are sensitive data transmissions encrypted? *FISCAM AC-3.2*								
16.2.15 Is access to tables defining network options, resources, and operator profiles restricted? *FISCAM AC-3.2*								
16.3. Critical Element: If the public accesses the system, are there controls implemented to protect the integrity of the application and the confidence of the public?								

NOTES:

17. AUDIT TRAILS

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems. The following questions are organized under one critical element. The levels for the critical element should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Audit Trails *OMB Circular A-130, III FISCAM AC-4.1 NIST SP 800-18*								
17.1. Critical Element: Is activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated?								
17.1.1 Does the audit trail provide a trace of user actions? *NIST SP 800-18*								
17.1.2 Can the audit trail support after-the-fact investigations of how, when, and why normal operations ceased? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
17.1.3 Is access to online audit logs strictly controlled? *NIST SP 800-18*								
17.1.4 Are off-line storage of audit logs retained for a period of time, and if so, is access to audit logs strictly controlled? *NIST SP 800-18*								
17.1.5 Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail? *NIST SP 800-18*								
17.1.6 Are audit trails reviewed frequently? *NIST SP 800-18*								
17.1.7 Are automated tools used to review audit records in real time or near real time? *NIST SP 800-18*								
17.1.8 Is suspicious activity investigated								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
and appropriate action taken? *FISCAM AC-4.3*								
17.1.9 Is keystroke monitoring used? If so, are users notified? *NIST SP 800-18*								

NOTES:

LIST OF REFERENCES

[AUS] Industrial Systems Automation and Security: An "Electronic Pearl Harbor?" by John Best http://www.giac.org/practical/john_best_gsec.doc Accessed July 2004

[BLACKOUT] "Blackout: The Conspiracy Theory" by Jim Wilson http://popularmechanics.com/science/military/2003/1/blackout_conspiracy/index.phtml Accessed July 2004

[DITSCAP] http://iase.disa.mil/ditscap/ditsprimer.ppt Accessed September 2004

[DODENERGY] Department of Defense Fiscal Year 2000 Annual Energy Management Report http://64.233.167.104/search?q=cache:MIRja_tzTckJ:www.acq.osd.mil/ie/irm/Energy/energymgmt_report/fy00/Annual%2520Energy%2520Management%2520Report%2520FY%25202000.pdf+scada+maxwell+afb&hl=en Accessed September 2004

[GAO] GAO sees threats to industrial systems http://www.fcw.com/fcw/articles/2004/... June 15, 2004

[GIANLU] "New vulnerabilities to DoS attacks in 802.11 networks" Gianluigi Me, PhD and Dr. Francesco Ferreri http://www.wi-fitechnology.com/Wi-Fi_Reports_and_Papers/DoS-attacks/defining_DoS_attacks.html Accessed September 2004

[HSPD-7]Homeland Security Presidential Directive http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html Accessed June 2204

[INEEL] Testbed Asset Description https://collaboration.inel.gov/CSSTC/index.cfm?fuseaction=CyberTesting&fuse= Accessed September 2004

[ISA] "Integrating Electronic Security into the Manufacturing and Control System Environment" ISA-TR99.00.02-2004 The Instrumentation, Systems, and Automation Society (ISA)

[McDonnell] Statement of James F. McDonnell Director, Protective Security Division, Information Analysis and Infrastructure Protection Directorate Department of Homeland Security Before the Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census U.S. House of Representatives March 30, 2004

[NIJ] **"**A Method to Assess the Vulnerability of U.S. Chemical Facilities**"** Study conducted by Sandia National Labs for the National Institute of Justice http://www.ncjrs.org/pdffiles1/nij/195171.pdf Accessed August 2004

[NIST800] NIST Special Publication 800-26 Self-Assessment Guide for Information Technology Systems **http://csrc.nist.gov/publications/nistpubs/** Accessed August 2004

[NTSB]*PipelineAccidentReport* PipelineRupture and Subsequent Fire in Bellingham,Washington June 10, 1999 NTSB Number PAR-02/02

[PDD63] Protecting America's Critical Infrastructures Presidential Decision Directive 63 http://www.fas.org/irp/offdocs/pdd/pdd-63.htm Accessed August 2004

[WIFI] "Ask an Expert: WiFi for SCADA? Robert Schmidt http://www.powersystem.org/media/documents/pdf/Ask%20an%20Expert%20-%20WiFi%20for%20SCADA.pdf Accessed September 2004

[OMNIV] "The SCADA Communications Quandary" by Bob Conner; Omnivergent Communications

[PETERS] NERC CIP Committee Control Systems Security Working Group Top 10 Vulnerabilities of Control Systems 'DRAFT' by Michael Peters

[ROCK] Configured Panel U.S. Navy Certifications http://files.awdm.com/e-files/ra/gmse00/gmse00-ap001a-en-p.pdf Accessed August 2004

[SAFIRE] "The Farewell Dossier" article for the New York Times dated February 2, 2004 by William Safire http://www.cs.hut.fi/Studies/T-106.530/2004/lectures/NYTimes%20-%20The%20Farewell%20Dossier.pdf

[SPP] System Protection Profile - Industrial Control Systems Version 1.0 Prepared for the National Institute of Standards and Technology by Decisive Analytics 14 April 2004

[WASHPT] *Cyber-Attacks by Al Qaeda Feared* by Barton Gellman June 27, 2002; Page A01. http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26 June 16, 2004

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Susan Alexander
   National Security Agency
   Fort Meade, MD

4. George Bieber
   OSD
   Washington, DC

5. RADM Joseph Burns
   Fort George Meade, MD

6. Marine Corps Representative
   Naval Post Graduate School
   Monterey, CA

7. Director, Training and Education
   MCCDC, Code C46
   Quantico, VA

8. Director, Marine Corps Research Center
   MCCDC, Code C40RC
   Quantico, VA

9. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
   Camp Pendleton, CA

10. Deborah Cooper
    DC Associates, LLC
    Roslyn, VA

11. CDR Daniel L. Currie
    PMW 161
    San Diego, CA

12. LCDR James Downey
NAVSEA
Washington, DC

13. Dr. Diana Gant
National Science Foundation

14. Richard Hale
DISA
Falls Church, VA

15. LCDR Scott D. Heller
SPAWAR
San Diego, CA

16. Wiley Jones
OSD
Washington, DC

17. Russell Jones
N641
Arlington, VA

18. David Ladd
Microsoft Corporation
Redmond, WA

19. Dr. Carl Landwehr
National Science Foundation
Arlington, VA

20. Steve LaFountain
NSA
Fort Meade, MD

21. Dr. Greg Larson
IDA
Alexandria, VA

22. Penny Lehtola
NSA
Fort Meade, MD

23. Ernest Lucier
Federal Aviation Administration
Washington, DC

24. CAPT Sheila McCoy
Headquarters U.S. Navy
Arlington, VA

25. Dr. Vic Maconachy
NSA
Fort Meade, MD

26. Doug Maughan
Department of Homeland Security
Washington, DC

27. Dr. John Monastra
Aerospace Corporation
Chantilly, VA

28. John Mildner
SPAWAR
Charleston, SC

29. Keith Schwalm
Good Harbor Consulting, LLC
Washington, DC

30. Dr. Ralph Wachter
ONR
Arlington, VA

31. David Wennergren
DONCIO
Arlington, VA

32. David Wirth
N641
Arlington, VA

33. Daniel Wolf
NSA
Fort Meade, MD

34. CAPT Robert Zellmann
CNO Staff N614
Arlington, VA

35. Dr. Cynthia E. Irvine
Naval Postgraduate School
Monterey, CA

36. Deborah Shifflett
Naval Postgraduate School
Monterey, CA

37. Karen Burke
Naval Postgraduate School
Monterey, CA

38. Dennis Hart
Naval Postgraduate School
Monterey, CA